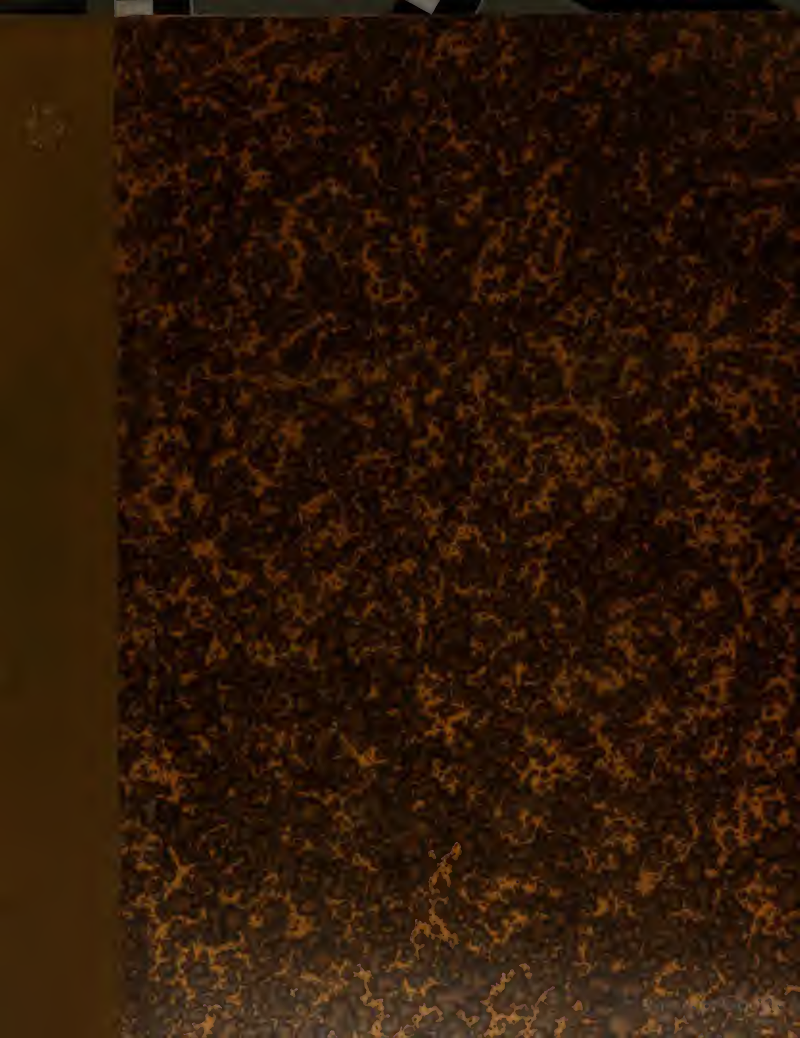




LEONHARDI EULERI

OPERA MINORA COLLECTA

I.

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

COLLECTAE.

AUSPICIIS

ACADEMIAE IMPERIALIS SCIENTIARUM PETROPOLITANAE

EDIDERUNT

AUCTORIS PRONEPOTES

Dr. P. H. FUSS

ACADEMIAE PETROPOLITANAE PERPETUO A SECRETIS

ET

NICOLAUS FUSS

MATHESEOS PROFESSOR IN GYMNASIO PETROPOLITANO LARINENSI.

INSUNT

PLURA INEDITA

TRACTATUS DE NUMERORUM DOCTRINA CAPITA XVI ALIAQUE.

TOMUS PRIOR.



PETROPOLI.

Typis ac impensis Academiae Imperialis scientiarum.

1849.

IMPERATORI AUGUSTISSIMO

NICOLAO PRIMO

CONSECRATUM.

PROOEMIUM.

Cum anno 1843, epistolas Eulerianas editurus [1], catalogum omnium summi illius Geometrae operum, quem jam dudum in usum meum comparaveram, editioni subjungere constituissem, facta et comparatione et accurata disquisitione, non solum eo perveni, ut novus ille catalogus (*B*), ex arte redactus, plenior evaderet illo (*A*), quem pater, anno 1783 vitam Euleri scribens, publici juris fecerat [2], sed ejus ope in fasce manuscriptorum Euleri, qui in tabulario academico servatur, opus detexi hucusque ineditum, inscriptum: *Astronomia mechanica*. De cujus inventi magno pretio cum dubitari non posset, rei detectae nuncium viris mathematicis mittere festinavi [3]. Aestate ejusdem anni Parisiis, in Bibliotheca regia, alterum vidi Euleri autographum, quod a Lagrangio donum acceperat Lacroix, venditum deinde ex hereditate hujus viri et tractatum continens inscriptum: *Considérations sur quelques formules intégrales dont les valeurs peuvent être exprimées, en certains cas, par la quadrature du cercle*, paginas 32 in 4to et 55 paragraphos complectens. Cum extemplo intellexissem, opusculum hoc ineditum esse, benevolo officio custodis Bibliothecae Hasii, viri in literis graecis celeberrimi, apographum hujus commentationis mihi parari curavi. Ut quidem utriusque libri cognitio mihi inexspectata fuerat, ita deinde nullus dubitavi, etiam fascem evolvere et perscrutari manuscriptorum Euleri, ab heredibus ejus asservatorum, sed quae antehac examine vix digna erant judicata, cum operum editorum apographa in usum preli confecta haberentur. Quantopere vero miratus sum, cum in hoc fasce copiam commentationum incognitarum, manu Auctoris scriptarum, et fragmenta operum majorum cognoscerem, quae omnia Auctoris immortalis ingenium prae se ferebant. Vir ille ex longo

(1) Correspondance mathématique et physique de quelques célèbres Géomètres du XVIII siècle etc. St.-Pétersb. 1843. T. I. II. 8vo.

(2) Eloge de Léon. Euler, par Nicolas Fuss. St.-Pétersb. 1783. 4to.

(3) Correspondance T. I. p. CXIX.

60 annorum somno resurrexisse videbatur, scilicet decimo quarto post anno quam Academia ultimas doctrinae Eulerianae copias, quas jam omni exspectatione majores reliquerat, publici juris fecisse putaverat, eo ipso pietate erga summum Sodalem quodammodo defuncta. Non enim est quod moneam Academiam nullam horum ineditorum notitiam habuisse, quae ex parte majori imperfecta, nec producta, nec diariis academicis inscripta erant.

Laetissimo animo die 8 Martii 1844 de inventis referens, ipsa autographa Academiae tradidi, ita tamen, ut censerem etiam haec opuscula publici juris fieri debere, et hanc esse occasionem animadverterem, quae ad editionem novam omnium Euleri operum suo loco proponendam induceret.

Propositum hoc omnium consensu approbatum eo deinde perduxit, ut ex sodalibus Academiae, doctrinas mathematicas, astronomicas et physicas profitentibus eligerentur, qui rem accuratius cognoscerent. Die 6 Aprilis ab Academia rogatio illustri est oblata Praesidi, jam antea sibi rem summopere cordi fore pollicito. In literis, quae rogationem comitantur, haec inter alia leguntur:

«Cum ante hos decem fere annos in coemeterio Dei Matri Smolenskianae sacro, lapis «sepulcralis in terram demersus et caespite opertus ipsumque Euleri sepulcrum denuo «detectum esset, Academia monimentum perennius suis impensis erigere, et ita locum, ubi «corpus Viri immortalis jaceret, posteritati indicare constituit. Sed nunc de alio monimento «eoque digniore res est, majores vero poscente opes, quam quas Academia possidet, quod «et pietati apte responderet, et decori foret atque usui diuturno. Hoc monimentum, quod «etiam ad veram Rossiae in literis gloriam promovendam valebit, est

«editio completa omnium operum Viri illius, quem Academia Petropolitana inde a «prima origine quinquaginta amplius annos suum fuisse gloriatur».

Verum enimvero nimis magna moliti sumus, cum inde ab initio propositum esset, ut non solum commentationes Euleri colligerentur, accessu pleraeque difficillimae, quae in variis Societatum eruditarum Actis dispersae sunt [1], sed etiam omnes ejus libri majores reciperentur, qui vel hodie apud bibliopolas prostant, vel inter libros veteres veneunt, atque in plures linguas recentiores versi occurrunt. Quod operum corpus ita adornare in mente erat, ut partes variae, secundum certas doctrinas collectae, in sectionibus ita constitutis ordine chronologico exhiberentur. Totum opus, decore, quamvis sine luxuria typographica, exemplaribus sexcentis edendum, decursu 10 annorum ut ad finem perduceretur in votis fuerat [2]. Respecto vero et laboris typographici et chartarum majore apud nos pretio,

(1) Acta Petropolitana sola plus quingentos Euleri continent tractatus. In actis Berolinensibus reperiuntur 120, in Parisiensibus 17, in Lipsiensibus 10, in Taurinensibus 6, rel.

(2) Computatio probabilis volumina 25 indicabat, quorum singula 80 plagulas impressas, seu paginas 640 in 4to maj. continerent. Quotannis itaque 200 plagulae fuissent prelo perficiendae, seu 4 quavis hebdomade.

etiamsi nulla foret editorum remuneratio, pro labore arduo in ordinanda materia, in inspiciendo opere typographorum et in corrigendis plagulis[1] impendendo, quem laborem editores in fronte hujus libri citati se gratuito suscepturos polliciti erant, mox apparuit, talem editionem postulare sumtus, quantos ex aerario publico spes parva erat tum temporis impetrandi.

Hac mente etiam Illustrissimus eruditionis publicae Minister (Academiae Praeses) respondit, rem neutiquam per se recusans, sed potius in tempus magis secundum differens, probata ipsius et dignitate et utilitate.

Si rogatio omnino rejecta fuisset, Academia absque dubio consilium cepisset Inedita suis impensis protinus edendi. Nunc vero prudentia ad exspectationem adhortata est. Novis deinde duobus annis elapsis, cum tempora secundiora etiamnum desiderarentur, viri vero mathematici de dilatione quererentur, Academia, secundum propositum meum, *Operum minorum collectorum* editionem de suo parare constituit, cujus exordium forent *tractatus arithmetici.* Magni conaminis primis fundamentis ita jactis, spes aderat fore, ut, applaudentibus omnium gentium viris mathematicis, etiam publica munificentia opus inceptum adjuvaret. Secundum hujus editionis consilium, abstinemus in praesens ab operibus majoribus denuo imprimendis, quae ut minoris sunt necessitatis, ita editionis sumtus non mediocriter augerent.

Caussae, cur commentationibus arithmeticis primum assignemus locum, sunt hae: 1. quod re vera in nexu naturali doctrinarum mathematicarum Arithmetica principium est; 2. quod inter partes majoris momenti ambitum habet non nimium, et faciliori negotio a reliquis doctrinis sejungi potest; 3. quia denique plura Inedita ad Arithmeticam pertinent, et majora et minora, quibus edendis jam ansa praebetur. Experientia insuper, quam in hac parte edenda nacti fuerimus, futuram editionem commentationum ad doctrinas altiores et graviores pertinentium suo tempore egregie adjuvabit.

Haec sufficient de delecta duorum voluminum nunc in lucem editorum materie. Antequam vero ad consilium accuratius exponendum progrediamur, quod secuti sumus et in materie ordinanda et per totum incepti operis decursum, revertamur ad Ineditorum copiam, qualis nunc est, anno quarto postquam primum de iis nuncium viris doctis misimus. Etenim et per se est gravissimum et ad eventum incepti nostri magni momenti videtur, viros mathematicos nosse, quantas copias ex fonte doctrinae et ingenii Euleri etiamnum exspectare liceat, quamquam alimento caruisset per binas jamjam aetates.

En recensus completus tractatuum detectorum, quos ineditos esse mihi constat.

(1) Etenim ipsae editiones primae plerumque erroribus typographicis scatent.

A. NUMERORUM DOCTRINA. ANALYSIS INDETERMINATA.

1. *De quadratis magicis.*

(Exhib. 1776 d. 17 Oct. §§ 1—32, pagg. 23. Huj. Collect. comment. XCII. T. II. p. 593).

2. *Recherches sur deux problèmes de l'Analyse de Diophante:*

1. *Trouver trois nombres carrés tels, que la somme de deux moins le troisième fasse un nombre carré.* (§§ 1—49).
2. *Trouver quatre nombres inégaux et entiers tels, que la somme de deux fasse toujours un carré.* (§§ 1—14). (Exhib. 1781 d. 1 Mart. pagg. 40).

3. *Supplément à ce dernier problème.*

(Exhib. 1781 d. 23 Apr. §§ 1—5 et 1—28, pagg. 8. NN. 2 et 3 insertae sunt huj. Collect. T. II pagg. 603 et 617 sub NN. XCIII et XCIV.)

Commentationes hae tres in diariis academicis dictis diebus lectae citantur. N. 1 manu adjuncti Golovini scripta in fronte habet verba: *Auctore* Leonhardo Eulero. In catalogo *B* pag. LXIV haec commentatio deperdita est dicta. NN. 2 et 3 (catalogi *B* pag. LXIII. 754 et 755). Hi tractatus duo manu Wilbrechtii, alterius discipuli Euleri, sunt exarati. Inscriptum in fronte invenies: *Calculé, sous la direction de M.* L. Euler, *par* Alexandre Wilbrecht. Seriori vero manu haec inscriptio correcta est, ita ut remanserint sola verba *par M.* L. Euler. Omnes tres commentationes in catalogo *A*, vitae Euleri adjecto, citatae reperiuntur(1). Non tamen mirandum est eas tum esse rejectas, cum selectio fiebat eorum tractatuum, qui deinceps, inde a morte auctoris usque ad annum 1830, in Commentariorum voluminibus publici juris sunt facti(2). Etenim in fronte N. 1 a patris, N. Fussii, manu verbum *supprimatur* adjectum videmus, quo indicasse videtur hanc commentationem, sicut NN. 2 et 3, negligentiis quibusdam digestionis laborare, quamquam nullum de origine esset dubium. Hi enim tres tractatus, quamvis formae minus perfectae sunt, a discipulis datae, nihilominus in argumento tractando artis indicant ipsum principem. Quodsi igitur olim imperfectiores judicabantur, quam quae Commentariis insererentur, attamen in completa operum editione deesse non debent. NN. 2 et 3 vero nova formae digestione egebant, antequam ederentur, quam doctissimus Tschebyschevius(3) non minus benevole quam apte perfecit.

4. *Considerationes circa Analysin Diophanteam.*

(§§ 1 ad 31, pagg. 24. Huj. Collect. comment. XC. T. II. p. 576).

5. *Theorema arithmeticum ejusque demonstratio.*

(pagg. 8, incompl. Hujus Collect. comment. XCI. T. II. p. 588).

N. 4 et 5 *Autographa* sunt munda. N. 4. Chirographum, de cujus fide nullum est dubium, hanc commentationem ab Eulero aut adolescente, aut seni conscriptam esse docet. Ex ipso vero argumento lector mox intelliget, auctorem tum temporis in rebus ita tractandis versatissimum fuisse, unde tractatum hunc ex serioribus esse colligimus, fortasse ex postremis, quos, oculis jam captus, ipse redegerit et rescripserit.

6. Commentationis fragmentum non inscriptum.

(§§ 27 ad 34, 35^{ti} initium, deinde §§ 49 ad 55).

Plagula dimidia *Autographi* mundi commentationis cujusdam majoris arithmeticae, quae de ratione inter triangulorum latera egisse videtur, quorum areae rationaliter exprimi possunt. Cum paginae 3^{a} et 4ta hujus fragmenti duorum problematum solutiones exhibeant completas, quorum alterum saltem in scriptis Eulerianis alibi non invenitur, non ingratum fore arbitrati sumus, si totum hoc fragmentum, attentione omnino non indignum, inter appendices Tomi II collocetur.

(1) N. 2. Haec commentatio, ut opus extraneum, more academico duobus sodalibus ad judicium de ea ferendum est tradita, sed qui nunquam judicium protulerunt. N. 3 vero eodem modo inscripta, in diariis academicis distinctis verbis opus *Eulerianum* vocatur.

(2) Euleri tractatus postumi 189 in tribus seriebus Commentariorum Petropolitanorum reperiuntur, quae sunt *Acta* a T. IV. P. II usque ad finem, *Nova Acta* pro 1784—1802 voll. 15, et *Memoires de l'Academie* etc. 1809—1830 voll. 11. Alii 29 ad paranda Vol. II *Opuscul. analyt.* nec non Vol. IV *Institut. Calcul. integr.* edit. 1792—1794 inservierunt.

(3) Hujus Geometrae doctrinam opus de theoria numerorum mox edendum testabitur.

7. *Tractatus de numerorum doctrina capita XVI.* (§§ 1—587, pagg. 112.)

N. 7 cum hujus collectionis partem faciat, ad capitum summas cognoscendas, Index rerum Voluminis secundi est evolvendus.

B. GEOMETRIA.

8. Tractatus *autographus*, non inscriptus. (§§ 179, pagg. 104 cum figuris.)

Usum continet calculi differentialis in linearum curvarum doctrina. In involucro elenchus capitum:

Cap. 1. De calculo differentiali ad lineas curvas applicato in genere. §§ 1—35.
Cap. 2. De tangentibus linearum curvarum. §§ 1—36.
Cap. 3. De tangentibus linearum curvarum, quae per alias lineas curvas utcunque determinantur. §§ 1—50.
Cap. 4. De tangentibus curvarum in certis locis inveniendis. §§ 1—54.
Cap. 5. De inventione ramorum in infinitum extensorum. §§ 1—4 (incompl.).
Cap. 6. De curvedine linearum curvarum. (prorsus deest).

N. 8 sine dubio est initium tertiae illius sectionis *Institutionum Calculi Differentialis*, quam designat Eulerus in variis ipsius operis locis (Inst. C. D. pars II Cap. 11 §§ 282. 283. 286). In judicio de Calculo differentiali »a mathematico experto, qui nomen indicare vetuit«, lato, quod Formeius, Academiae Berolinensis Secretarius, in libro edidit: *Nouvelle Bibliothèque germanique* T. XII p. 269, haec verba reperiuntur, in quibus de tertia sectione sermo est: »*C'est un ouvrage particulier dans lequel l'Auteur donne l'application du calcul infinitésimal à la Géometrie, mais qui n'a point encore paru*«(1).

C. CALCULUS SINUUM.

9. *Enodatio insignis cujusdam paradoxi circa multiplicationem angulorum.* (*autogr.*) (§ 1—34, pagg. 22.)

D. CALCULUS PROBABILIUM.

10. *Vera aestimatio sortis in ludis.* (*autogr.*) (pagg. 7.)

11. *Réflexions sur une espèce singulière de loterie, nommée loterie génoise.* (*autogr.*) (§§ 1—28, pagg. 23.)

Tractatus hic regis Friderici II mandato originem debet. Roccolini quidam, italus, rogationem de hac sortium alea in Borussiam introducenda ad magnum miserat regem, qui Euleri de hac re petebat judicium. Literae regiae et Geometrae responsum (primum nempe exemplum manu sua conscriptum) in collectione reperiuntur, quam Academiae dono obtuli, et una cum alio mandato simili anni 1763 et responso in Epistolarum tertio volumine mox edendo legentur. Tractatus hic noster problema doctissime tractat et omnino differt tam a relatione ad regem missa, quam a commentatione N. 300 catalogi *B*.

E. CALCULUS INTEGRALIS.

12. *Considérations sur quelques formules intégrales dont les valeurs peuvent être exprimées, en certains cas, par la quadrature du cercle.* (§§ 1—55, pagg. 32.)

Autographum, quod inspexi, in Bibliotheca regia parisina servatur, ut supra dixi. Insuper vero apographum decurtatum detexi et accurate confectum, Joh. Alb. Euleri manu exaratum, quod formularum in singulis paragraphis exhibitarum recensum dat.

(1) Ex literis Cl. Jacobii ad me missis.

13. *De trajectoriis reciprocis.* (*autogr.*)

(Exhib. Berol. 1746 d. 23 Junii, pagg. 32.)

14. *Solutio problematis difficillimi ex methodo tangentium inversa.*

(Exhib. Petrop. 1774 d. 12 Maji, §§ 1—7, pagg. 3.)

Haec commentatiuncula a Nic. Fussio digesta et scripta inter prima specimina diligentissimi et utilissimi illius discipuli Euleriani mihi ponenda videtur, qui anno demum praecedenti 1773, 19 annos natus, in magni Praeceptoris societatem venit. (Vide *Correspond.* I p. XLI seq.). Caussa in promtu est, cur hoc opusculum, sicut N. 1, sepositum sit et ineditum manserit.

15. *Solutio problematis in Actis Lips. A.* 1745 *M... propositi.* (*autogr.*)

(§§ 1—13, pagg. 8, incompl., figurae desunt.)

Problema idem est catoptricum, ab Eulero ipso, ut jam constat, in Actis Erud. 1745 mathematicis propositum, deinde solutum ab ipso auctore, primum in Actis Erud. 1746, nulla adjecta expositione analytica, posthac copiosius 1748. (Vide infra Emendationes catalogorum *A* et *B* sub N. 9 et 10). Etiam in epistolis cum Goldbachio mutuis (*Corresp.* I p. 341, 355, 358 et saepius) pluries de hoc problemate sermo est. Nostra commentatio solutionis primus ille conatus, deinde rejectus videtur esse, cujus in Actis Erud. 1748 p. 46 fit mentio.

16. *De invenienda linea, quae cum data juncta efficiet omnes descensus isochronos.*

(Exhib. Petrop. 1732 d. 10 Mart. §§ 1—18, pagg. 12, cum 2 figuris.)

Apographum manu ipsius Euleri signatum: »*Autographo congruum reddidit* Leonh. Euler«.

F. MECHANICA.

17. *Statica.* (*autogr.*) (§§ 1—211, pagg. 68, cum figuris ad marginem delineatis.)

Notiones praeviae §§ 1—18. *Sectio prima.* De aequilibrio potentiarum puncto applicatarum §§ 19—211.

18. *Vera vires existimandi ratio.* (*autogr.*) (§§ 1—20, pagg. 12.)

19. *Von der Kraft der Rammen, Pfähle einzuschlagen.*

(Exhib. Petrop. 1772 d. 18 Maji, §§ 1—35, pagg. 48.)

Est rudimentum a W. L. Krafftio conscriptum, lectu facile. In diariis Academiae Petropolitanae, die 18 Maji 1772, una cum 12 aliis citatur commentationibus, quae omnes, incendio domus ereptae et restitutae, ab Eulero oblatae erant Academiae[1]. Ex quo numero, undecim commentationes in Actis sunt editae. Nostra commentatio N. 19 vero in tabulario est deposita ad usum seriorem. Alia commentatio, decima tertia, cui germanice inscriptum erat: *Anweisung zu der sogenannten Delisle'schen Projection der Landkarten*, collegio geographico tradi placuit, at postea retractata in catalogo *B* sub N. 338 occurrere videtur.

20. *De oscillationibus annulorum elasticorum.* (*autogr.*)

(§§ 1—11, pagg. 5, cum figuris in margine delineatis.)

21. *Recensio litterarum a Cl.* Daniele Bernoullio *Basilea d.* 28 *Oct.* 1735 *ad me datarum, una cum annotationibus meis.* (*autogr.*)

(Pagg. 8, cum figura in margine delineata.)

Epistolam Bernoullii, de qua hic agitur, invenies in *Corresp.* T. II. pag. 427 ad 430.

(1) Tota nostra manuscriptorum Eulerianorum copia, in ejusdem incendii turba, sine ordine in fascem collecta et flammis erepta fuisse videtur; ita enim et confusio partium et multorum tractatuum manca conditio facile explicantur. Nonnulli nimirum tractatus nonnisi operose et per partes colligi poterant; plurium restitutio perfecta feliciter successit, alii incompleti manserunt. Ad hos, non vero omnes, supplendos, apographa, quae in Academia Berolinensi servantur, optimo cum successu inserviebant, uti infra ostendemus.

22. *Dissertation sur le mouvement des corps enfermés dans un tube droit, mobile autour d'un axe fixe.* (*autogr.*)

(§§ 1—49, pagg. 50, figg. 3 in duabus tabulis.)

23. *De motu corporum in tubo rectilineo, mobili circa axem fixum per ipsum tubum transeuntem.* (*autogr.*)

(§§ 1—33, pagg. 16, figurae 6 desunt.)

24. *De motu corporum in tubis circa punctum fixum mobilibus.* (*autogr.*)

(§§ 1—24, pagg. 14, figurae 5 desunt.)

25. *De motu corporum super superficiebus mobilibus.* (*autogr.*)

(§§ 1—44, pagg. 16, figurae 11 desunt.)

26. *De motu corporum circa punctum fixum mobilium.* (*autogr.*)

(§§ 1—76, pagg. 32, cum 6 figuris in duabus tabulis.)

27. *Principia pro motu sanguinis per arterias determinando.*

(Exhib. Petrop. 1775 d. 21 Dec. §§ 15—43, pagg. 15, figurae 3 in una tabula.)

Commentatio a Nic. Fussio digesta et scripta, hucusque inedita, quia §§ 1 ad 14 desunt.

G. ASTRONOMIA.

28. *Astronomia mechanica.* (*autogr.*)

(§§ 1—219, pagg. 181, cum 20 figuris in quatuor tabulis.) Elenchus capitum:

Cap. I. De viribus, quibus corpora coelestia sollicitantur. §§ 1—60.
Cap. II. De motu duorum corporum sphaericorum se mutuo attrahentium. §§ 61—109.
Cap. III. Aliae investigationes motus duorum corporum sphaericorum. §§ 110—127.
Cap. IV. De motu duorum corporum, quorum alterum tantum est sphaericum. §§ 128—149.
Cap. V. Determinatio motus corporis, quando inter vires, quibus sollicitatur, una ad punctum fixum tendens quadrato distantiae ab eo est reciproce proportionalis, reliquae vero vires prae illa sunt valde parvae. §§ 150—179.
Cap. VI. De motu trium corporum sphaericorum se mutuo attrahentium in genere. §§ 180—197.
Cap. VII. De perturbatione motus momentanea a vi quacunque sollicitante oriunda. §§ 198—219.
Digressio, qua effectus cometae A. 1759 expectati in motu Terrae perturbando investigatur

29. *Recherches des inégalités causées au mouvement des planètes par des forces quelconques.* (*autogr.*) (§§ 1—37, incompl., pagg. 32, figurae 2 desunt.)

30. Commentatio *autographa* non inscripta.

(§§ 1—13, pagg. 21, cum 4 figuris in duabus tabulis.)

Continet solutionem duorum problematum sequentium: 1. *Si corpus sphaeroidicum, ex materia homogenea conflatum, attrahatur ad centrum virium, cujus vis sit reciproce proportionalis quadratis distantiarum, invenire medium directionem, secundum quam hoc corpus urgebit.* (§§ 1—12). 2. *Determinare motum axis Terrae, quatenus is a vi Solis perturbatur, seu nutationem axis Terrae a vi Solis oriundam definire.* (§ 13.)

31. *Tabula aequationis meridiei, ex duabus aequalibus Solis altitudinibus, ante et post meridiem observatis, in minutis tertiis temporis computata, pro singulis gradibus declinationis*

Solis ab intervallo observationum unius horae usque ad octodecim, ad elevationem poli in Observatorio Petropolitano, quae est 59° 57'.

(Pagg. 7 fol. transv.)

32. *Nouvelles tables astronomiques pour calculer la place du Soleil.*

(Exhib. Berol. 1744 d. 9 Apr., §§ 1—38, pagg. 32, cum 6 figuris in una tabula.)

Autographi hujus, aliena manu (fortasse Formeii) in dictione correcti, tomus I. Actorum Berolinensium breviarium exhibet. Alio jam loco indicavimus, regnante Friderico magno, linguam gallicam non solum publice in Academia Berolinensi obtinuisse, sed etiam eam fuisse, qua in scriptis academicis uti viris doctis injunctum erat. Cum nondum linguae facilitatem possideret, Eulerum ipsum multum temporis pretiosissimi versionibus faciendis impendisse constat. (Vide, in fine hujus enumerationis, commentationum, lingua gallica in Actis Berolinens. publici juris factarum, prima exempla latine conscripta et inedita). Ex quo fonte derivantur correctiones multae in manuscriptis Berolinensibus hujus prioris periodi, aliena scriptae manu, quae ad dictionem emendandam tendent. Seriori tempore, cum usum linguae adeptus esset, Eulerum commentationes primitus gallice scripsisse constat.

33. *De emendatione tabularum lunarium per observationes eclipsium Lunae.* (*autogr.*)

(§§ 1—30, pagg. 20, cum 2 figuris in tabula una.)

34. Tria capita de motu Lunae: *Cap. De vero loco nodi atque vera inclinatione orbitae lunaris ad eclipticam* (§§ 1—16). *Cap. De diametris apparentibus motuque horario vero Solis ac Lunae in eclipsibus lunaribus* (§§ 1—16). *Cap. De loco Lunae ex eclipsibus lunaribus determinando* (§§ 1—28). (*autogr.*)

(pagg. 32, figurae 2 ad caput ultimum pertinentes desunt.)

35. *De motu cometarum in orbitis parabolicis Solem in foco habentibus.* (*autogr.*)

(§§ 1—32, pagg. 24, cum 4 figuris in duabus tabulis.)

Scripta NN. 30 ad 35 an prius edita fuerint, nec ne? examen benevole instituit Collega doctissimus Peters, eaque nusquam prelo impressa esse invenit.

H. RES TORMENTARIA.

36. *Meditatio in experimenta explosione tormentorum nuper instituta.* (*autogr.*) (pagg. 6.)

I. PHYSICA.

37. *Anleitung zur Naturlehre, worinn die Gründe zu Erklärung aller in der Natur sich ereignenden Begebenheiten und Veränderungen festgesetzet werden.*

(§§ 1—161, pagg. 161, cum 24 figuris in tribus tabulis.) Elenchus capitum:

Kap. 1. Von der Naturlehre überhaupt. §§ 1—8.
Kap. 2. Von der Ausdehnung, als der ersten allgemeinen Eigenschaft der Körper. §§ 9—15.
Kap. 3. Von der Beweglichkeit, als der zweiten allgemeinen Eigenschaft der Körper. §§ 16—25.
Kap. 4. Von der Standhaftigkeit, als der dritten allgemeinen Eigenschaft der Körper. §§ 26—34.
Kap. 5. Von der Undurchdringlichkeit, als der vierten allgemeinen Eigenschaft der Körper. §§ 35—.
Kap. 6. Initium deest §§ —50.
Kap. 7. Von der Wirkung der Kräfte auf die Geschwindigkeit der Körper. §§ 51—61.
Kap. 8. Von der Wirkung der Kräfte auf die Richtung der Körper. §§ 62—68.
Kap. 9. Bestimmung der Bewegung eines Körpers, welcher von Kräften getrieben wird. §§ 69—76.
Kap. 10. Von der scheinbaren Bewegung. §§ 77—83.
Kap. 11. Allgemeine Grundregeln der Naturlehre. §§ 84—90.

Kap. 12. Von dem Unterschied der Körper in Vergleichung ihrer Ausdehnung mit der Standhaftigkeit. §§ 91 — 97.
Kap. 13. Von den besondern Eigenschaften der groben und subtilen Materie. §§ 98 — 104.
Kap. 14. Von dem Aether, oder der subtilen Himmelsluft. §§ 105 — 111.
Kap. 15. Von der Flüssigkeit. §§ 112 — 118.
Kap. 16. Von den verschiedenen Gattungen der Körper. §§ 119 — 125.
Kap. 17. Erklärung der Festigkeit der Körper. §§ 126 — 132.
Kap. 18. Von der Zusammendrückung und Federkraft der Körper. §§ 133 — 139.
Kap. 19. Von der Schwere und den Kräften, so auf die himmlischen Körper wirken. §§ 140 — 146.
Kap. 20. Von dem Gesetz des Gleichgewichts in flüssigen Materien. §§ 147 — 154.
Kap. 21. Von den Gesetzen der Bewegung flüssiger Materien. §§ 155 — 161.

Autographum lingua germanica conscriptum 161 paginas continet; plagula sexta deest. Suspicor opus hoc idem esse, de quo Gerh. Frid. Müllerus in historia manuscripta Academiae haec habet: »*Wegen eines Buches* Systema Physices, *so Hr. Prof.* Euler *verfertiget haben soll und wofür er den 14 September* (1731) 100 *R*°. *zur Belohnung bekommen, kann ich keine Erläuterung geben.*« Quid, num tam tenuis pretii invidia caussa exstitit, cur opus publici juris non sit factum eo tempore, quo utilissimum esse potuit? Sed etiam hodie fortasse libro huic in nonnullis saltem partibus, dignitas aliqua, non mere historica, est adscribenda.

38. *Théorie générale de la Dioptrique.*

(§§ 1 — 186, pagg. 48, cum 5 figuris in tabula una.) Praeter introductionem, continet *Considerationes* (seu capita) 7, quarum elenchus sequitur:

Consid. 1. Sur la réfraction d'une seule surface sphérique réfringente. §§ 1 — 29.
Consid. 2. Sur le passage des rayons par deux surfaces sphériques réfringentes. §§ 30 — 48.
Consid. 3. Sur le passage des rayons moyens par plusieurs surfaces réfringentes en général. §§ 49 — 58.
Consid. 4. Sur la route des rayons moyens qui, venant du centre de l'objet, passent par les bords de la première surface réfringente. §§ 59 — 70.
Consid. 5. Sur la route des rayons moyens qui, venant de l'extrémité de l'objet, passent par le milieu de la première surface. §§ 71 — 90.
Consid. 6. Sur les changements causés dans les images principales par la différente réfraction des rayons. §§ 91 — 112.
Consid. 7. Sur les télescopes et les microscopes en général. §§ 113 — 186.
1ère *Partie.* Examen d'un instrument dioptrique proposé. §§ 121 — 153.
2de *Partie.* Construction des instruments dioptriques. §§ 154 — 186.

39. Tractatus *autographus* non inscriptus.

(§§ 1 — 141, pagg. 88, cum 12 figuris in tribus tabulis). Elenchus capitum:

Chap. 1. Recherches générales sur la réfraction des rayons par les surfaces sphériques. §§ 1 — 44.
Chap. 2. Recherches sur le champ apparent par un nombre quelconque de surfaces réfringentes. §§ 45 — 63.
Chap. 3. Sur la confusion causée par la différente réfrangibilité des rayons. §§ 64 — 88.
Chap. 4. Sur le lieu le plus avantageux de l'oeil. §§ 89 — 102.
Chap. 5. Sur le grossissement et le degré de clarté. §§ 103 — 121.
Chap. 6. Sur la sensation que la confusion des images cause à l'oeil. §§ 122 — 135.
Chap. 7. Précis de la Théorie de toute la Dioptrique. §§ 136 — 141.

NN. 38 et 39 sunt *autographa* munda et absoluta, quae nunc inedita haberi debent, etiam judicio doctissimi collegae Petersii. Argumentum capitis in N. 39 ultimi transiisse videtur in commentationem, quam Acta Parisiensia anni 1765 habent, iisdem fere verbis inscriptam: *Précis d'une théorie générale de la Dioptrique.* Cujus vero elaboratio est prorsus alia, et ita discrepat a nota illa Euleri expositione, ut suspicari liceat laborem Eulerianum aliena manu licentius retractatum esse. Opus hoc in formam restitutum integram et genuinam absque dubio omnibus magni Geometrae cultoribus bene acceptum erit.

40. *Recherches pour servir à la perfection des lunettes.* (*autogr.*)

(Exhib. Berol. 1753 d. 26 Junii. §§ 1 — 169, pagg. 58.)

Hujus commentationis primam notitiam debebam epistolae cel. Mathematici Berolinensis Jacobii, qui ejus apographum in tabulario Academiae Berolinensis adservatum inspexit, *ineditum*, ut judicat.

Cum vero dubium sibi exstiterit, nonne hic tractatus idem esset, atque alter ex NN. 38 et 39, cel. Jacobius argumentum et formam autographi Berolinensis accurate indicavit. Ex quo cum statim mihi persuasum esset opus esse aliud, amicus doctissimus apographum se missurum benevole pollicitus est. Interea vero mihi contigit, manuscripta nostra nondum ordinata attentius et operose perscrutando, pedetentim colligere singulas plagulas ipsius hujus tractatus *autographi*, quem ita nunc pro majore omnino parte restitutum habeo, exceptis scilicet solis paragraphis 83—90, 93—96, 105—124, 141—156, 161—166, seu minus tertia parte totius operis.

41. *De amplificatione campi apparentis in telescopiis.* (*autogr.*)
(§§ 1—43, pagg. 23.)

42. *De la construction des microscopes.* (*autogr.*)
(§§ 1—85, pagg. 35, cum 3 figuris in una tabula)

43. *Constructio manometri, densitatem aëris quovis tempore accurate monstrantis.*
(Exhib. Petrop. 1780 d. 20 Nov., §§ 1—22, pagg. 13, cum 2 figuris in una tabula.)
Commentatio a Nic. Fussio digesta et conscripta, sicut NN. 14 et 27. Caussa, cur opusculum non sit editum, ea fuisse videtur, quod res obsoleta habebatur, cum digestio ipsa omni cura perfecta esset.

44. *Réflexions sur la détermination de la déclinaison de la boussole.* (*autogr.*)
(§§ 1—25, pagg 13, cum 6 figuris in una tabula.)

45. *Recherches sur la découverte des courants de mer.* (§§ 1—11, pagg. 6.)
Autographum hoc sex paginarum initium est responsi ad quaestionem ab Academia Parisina pro anno 1751 propositam, de maris fluminibus. Haec commentatio nunquam ad finem perducta esse videtur. Nam missa, sine dubio coronata fuisset.

K. VARIA.

46. *Meditatio de formatione vocum.* (*autogr.*) (pagg. 5.)

47. *Recensio dissertationis* (Cel. d'Alembert) *de Ventis*, ab Academia Berolinensi A. 1746 praemio ornatae. (*autogr.*) (pagg. 8.)

48. *Analyse de vingt-cinq pièces de concours sur les monades.* (*Autogr.*) (pagg. 8 in fol.)

49. *Examen libri, cujus titulus: Problemata mathematica quadraturam circuli cet. concernentia, per Matheseophilum.* Aug. Vind. A. 1733. (*autogr.*)
(Exhib. Petrop. 1735 d. 21 Febr., pagg. 7.)

Praeter hanc Ineditorum copiam, ex ducentis fere plagulis constantem, maxima parte manu Euleri conscriptis, quae totidem circiter plagulas typis expressas aequabunt, alia archetypa, attentione non indigna mihi videntur haec:

α. **Exempla prima latine conscripta commentationum, postea versione gallica editarum.**

50. *De vi percussionis ejusque mensura vera.* (§§ 1—18, pagg. 16.)
Autographum hoc plane congruit cum tractatu in T. I Actor. Berol. p. 21 edito, qui inscriptus est: *Sur la force de la percussion et sa véritable mesure*, N. 548 Catal. *B.* Sed exemplum nostrum latinum exit in § 16, dum in versione edita alii sequuntur paragraphi undecim.

51. *Disquisitio physica de causa caudarum cometarum et luminis borealis, itemque luminis zodiacalis.* (§§ 1—8, pagg. 8.)

Est primum exemplum *autographum*, sed incompletum commentationis N. 664 Catal. *B*.

52. *Dissertatio ad quaestionem de optimo modo anchoras attollendi (sur la meilleure construction du cabestan) ab Ill. Academia regia scientiarum Parisina pro A. 1739 propositam, cum annexo praemio 2000 libr.* (§§ 1—50, pagg. 66.) Epigrapho instructa:

Pressa momordit humum, superas nunc gaudet ad auras
Anchora judicio tendere nostra Tuo.

Archetypum *autographum* est commentationis in nostra Academia die 3 Julii 1738 depositae, sed cujus alind exemplum, anno insequenti Parisios missum, praemio ornatum, gallice editum est in collectione quam vocant: *Recueil des pièces couronnées.* Ubi vero cum nomen auctoris non indicatum esset, haec ipsa caussa fuisse videtur, cur opus hoc insigne vitae Eulerianae primum narratorem fugerit, et in utroque catalogo *A* et *B* desit. Archetypo nostro detecto, Eulerum auctorem fuisse ratum est. Vide infra Emendationes Catalogi *B*.

53. *De atmosphaera Lunae etc.* (pagg. $20^1/_2$.)

Apographum primi exempli latine conscripti commentationis, quae in Catal. *B* numerum fert 648. E scriniis Academiae Berolinensis.

β. Rudimenta prima, non exigui momenti, commentationum postea retractatarum et editarum.

54. *Autographum* mundum septem continens plagulas, inscriptione generali carens et in duabus sectionibus de curvarum arcubus, quadraturis aliisque quantitatibus transcendentibus comparandis agens. (§§ 1—70.)

Diu tractatum hunc ineditum esse censebam, sed postea reperi tres commentationes in T. VII Novor. Comment. exhibitas, quae sunt NN. 348. 352. 424 Catal. *B*, eadem habere argumenta, et ex nostro tractatu originem duxisse. Sed ipsum autographum est locupletius, cum insuper comparationem afferat arcuum hyperbolae et parabolae cubicalis primariae, quae comparatio in tribus commentationibus editis desideratur. Res vero, uti patet, maximi est momenti in theoria functionum ellipticarum, cujus fundamenta Eulerus jecit.

55. *De la plus avantageuse construction des lunettes à trois verres qui représentent les objets debout.* (*autogr.*) (§§ 1—52, pagg. 23.)

Hanc commentationem, Academiae Berolinensi die 3 Maji 1759 oblatam, posthac cum altera auctor confudit, quae ibidem die 2 Febr. 1758 lecta erat. Comparatio enim docet, teste Cl. Petersio, nonnullos nostri autographi paragraphos verbo tenus convenire cum tractatu Berolini edito, qui est N. 708 Catal. *B*. (Mém. de Berl. XX. 1764 p. 200.)

56. *De numeris amicabilibus.* (pagg. 19.)

Apographum est tractatus, redactionis prorsus diversae a commentatione eandem ferente inscriptionem, quae primum in *Opusculor. var. arg.* vol. 2 edita prodiit, et nunc quidem a nobis sub N. X in T. I hujus Collectionis nostrae pagg. 102 ad 145 reproducta invenitur. Hujus vero primae redactionis specimen, e tabulario Acad. Berolinensis depromtum, nobis minime ignotum fuit, quippe quod ipsius *autographi* fragmenta (§§ scil. 1. 2 et 8 ad 17) in nostra collectione reperiuntur. Introductio historica prae ceteris, ut et digressio de numeris perfectis, quam in seriore digestione non invenimus, nobis dignae videntur, quae supplementi loco publici fiant juris.

57. *Découverte d'une loi toute extraordinaire des nombres.*

(Exhib. Berol. d. 22 Junii 1747, pagg. 13.)

Apographum in tabulario Acad. Berol. servatum. Hanc ipsam commentationem, in catalogo nostro *B* sub N. 3 citatam, Cl. Gaussius quaerens alteram illam detexit, de qua infra res erit. Haec vero commentatio, ut docet Cl. Jacobius, est prima adumbratio tractatus serioris inscripti *Observatio de summis divisorum* (N. 17 Catal. *B* et in nostri libri T. I. N. XI p. 146). Quam itaque ejusdem viri Cel. auctoritate in opere nostro reproduci supervacaneum duximus.

58. *Sur les logarithmes des nombres négatifs et imaginaires.* (pagg. 19.)

59. *Détermination de l'effet d'une machine hydraulique inventée par M. le prof.* Segner *à Göttingue.*

(Exhib. Berol. d. 28. Sept. 1752.)

NN. 58. 59. Apographa e scriniis Acad. Berol. petita a commentationibus sub iisdem titulis catalogo *B* inscriptis NN. 189. 507 prorsus sunt diversa. Archetypi *autographi* N. 58 in nostra collectione sunt fragmenta quaedam, §§ scilicet 12—34 incl., pagg. 14 implentes.

γ. Epitomae copiosiores et ab Eulero ipso gallice conscriptae ex commentationibus primo anno Academiae Berolinensi oblatis.

60. *Pensées sur la lumière et les couleurs. (autogr.)*

(§§ 1—8, pagg. 8, cum 4 figuris in una tabula.)

Ipse tractatus, latine conscriptus una cum multis aliis ejusdem temporis, *Opusculis varii argumenti* edendis ansam praebuisse videtur. In qua collectione reperitur Vol. I p. 169—244 cum inscriptione: *Nova theoria lucis et colorum.* Argumentum ejus, brevissimis verbis, ab epitome nostra plane diversis, indicatum est in T. I Actor. Berol.

61. *Comparaison entre le choc et la pression.*

Autographum hoc, sic ut praecedens, eadem aliena manu, atque N. 32 Ineditorum, in dictione correctum, non est notitia illa brevis inscripta *sur le choc et la pression*, quae simpliciter refert de tractatu illo: *De la force de la percussion et de sa véritable mesure* (Mém. de Berl. I. 1745 p. 21). De hujus archetypo, latine conscripto, vide supra N. 50.

Non est quod multa verba de re faciamus, quae sponte animo nostro offertur, si horum supplementorum divitias cum catalogis operum et opusculorum Euleri antea cognitorum comparamus, et insuper reputamus, quantum temporis viri docti saeculi praeteriti, et Eulerus prae aliis, epistolarum commercio impendere debuissent. Inspiciamus solas epistolas ab Eulero ad Goldbachium, virum ingenii multo inferioris, scriptas, et facile aestimabimus, quantae doctrinae opes inesse debuerint in epistolis immortalis nostri Geometrae ad Danielem Bernoullium missis, quas deperditas esse aegre dolemus; quantae in commercio epistolarum cum Lagrangio et Delislio habito. Quas cum non interiisse exploratum sit, speramus fore, ut aliquando viris doctis communicare nobis detur. Mirabimur certe quomodo vita humana, non ad insolitum annorum numerum producta, ingentibus illis suffecerit doctrinae ingeniosae opibus procreandis. Id vero hoc loco verbis monendum est, ex copia Ineditorum ea solum scripta nos hucusque respexisse, quae sunt autographa munda ab ipso auctore sine dubio ea mente elaborata, ut publici fierent juris; rejectis primis illis delineationibus, plus minus

curatis, interdum inscriptiones prae se ferentibus, quales nusquam in catalogis occurrunt [1]. Has enim enumerationi nostrae non adjunximus, quippe quae alia occasione accuratius sunt examinandae. Insuper attendendum est, adversaria illa, quorum alio loco mentionem fecimus (*Corresp.* I p. XLIV seq.), sedulo perscrutandi otium hucusque nobis defuisse. Elucet superesse etiamnum spicilegium ex hisce manuscriptis foecundum. Id vero exploratum jam est, in iis nil inveniri, quod ad theoriam numerorum pertineat, praeter ea, quae in hoc nostro libro mathematicis offeruntur.

Exceptis NN 1. 2. 3. 14. 19. 27. 28. 43. 49, quae tabularia academica nobis obtulerunt, reliqua Inedita omnia ex possessione domestica depromta et a nobis deinde Academiae dono oblata sunt.

Jam supra indicavimus, in ordinanda editione eam nobis optimam videri rationem, ut in quavis doctrina systema aliquod accipiatur, in singulis vero ejus subdivisionibus ordo servetur chronologicus. Haec quidem ratio contra viri clarissimi Librii [2] opinionem pugnat, qui omnem rejicit operum selectionem, secundum argumenta institutam, et mixtionem deposcit disciplinarum, qualem ordo mere chronologicus per se efficit. Id solum concedimus, divisionem nimiam non commendari, et certos in ea perficienda fines esse ponendos, qui ex ipsis commentationum argumentis sunt petendi. Ordo enim chronologicus in singulis partibus eo placere debet, quod et naturalis est et quodammodo mentis Auctoris et viam et rationes indicat.

Alia quaestio haec identidem nobis se obtulit, utrum tractatus, qui quidem ad doctrinam aliquam systematis pertinere videantur, alii doctrinae adjiciendi sint, nec ne, si talis ipsorum est indoles, ut in hac demum alia doctrina foecunditatem adipiscantur, seu ipsius Auctoris, seu plerumque seriorum virorum laboribus et studiis. Rei maxime consentaneum nobis visum est, tali commentationi locum assignari non ex sequelis, sed secundum primum ipsius argumentum et secundum rationem, quam Auctor in argumento tractando secutus sit. Liceat hoc ambiguum exemplis nonnullis illustrare. Viri docti noverunt theorema illud Eulerianum

$$(1-x)(1-x^2)(1-x^3)(1-x^4)\ldots = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \ldots$$

maximi momenti esse in theoria numerorum, et cl. Jacobium ad nova duxisse theoremata speciosissima. Nihilominus, ne regulam propositam desereremus, nulli dubitavimus, quin commentationem 167 catalogi *B*, inscriptam: *Evolutio producti infiniti*

$$(1-x)(1-x^2)(1-x^3)\ldots\ldots$$

in seriem simplicem, in Opera arithmetica reciperemus, cum formae sit mere analyticae, nec sequelae illius ullum in ea inveniatur vestigium. Simili modo res ea singularis, quod problema,

(1) Ceterum inspicienti mox patebit haec chirographa, maxima parte, ad primam vitae Euleri periodum pertinere. Insunt nempe, inter alia, commentationes etiam Basileae ante A. 1727 conscriptae, cum notis manu praeceptoris, Joh. Bernoullii, margini adjectis etc., dum nostra Inedita fere omnia ad aetatem maturiorem et periodum imprimis Berolinensem (1741 — 1766) referenda sunt.

(2) Vide Recensionem Commercii epistolarum a me editi. *Journ. d. savants* 1844.

pag. 427 voluminis primi hujus Collectionis nostrae datum, usum peculiarem habet in doctrina de transformandis coordinatis, nullo modo movere nos potuit, ut commentationem hanc Geometriae adscriberemus. Hanc eandem regulam servaturi, locum ex primario argumento pendere, et auctoritate cl. Jacobii innisi, omnes commentationes geometricas, quae ita methodo ex analysi sublimiori petita excellunt, ut notiones geometricae fortuitam potius hujus methodi adhibendae occasionem praebuisse videantur, sine ulla haesitatione ad Calculum integralem ejusque in Geometria amplificanda usum retulimus. Si quis vero fortasse animadverterit nos in separatione commentationum, quae de integralibus ita dictis ellipticis agunt, legem datam omnino deseruisse, rei sane excusationem, si qua eget, in summa argumenti gravitate ipse inveniet.

In theoria vero numerorum systema, secundum quod commentationes Eulerianae, ad hanc analyseos mathematicae partem pertinentes, non minus commode et stricte quam libere subdividerentur, nullum reperimus, cum et Gaussii et Legendrii ordinationes ad hunc scopum minime quadrare viderentur. Aliud conamen commentationes segregandi secundum duas disciplinas: theoriam numerorum proprie sic dictam et analysin indeterminatam, non melius successit [1]. Quae res nos impulit, quamvis vituperationem timentes non prorsus fortasse injustam, ut simplicem amplecteremur in hac doctrina ordinem chronologicum, per totum hoc opus, exclusis Ineditis. Id vero propositum habebamus, dum opus typis excuderetur, omnem operam navare subsidiis parandis, quae, in fine libri addita, ad omnes particulas de eodem argumento tractantes facile inveniendas perducere possent.

Ad ordinem commentationum chronologicum recte constituendum, diaria academica omnia erant examinanda. Quem laborem uterque editorum seorsim subiit, ut ex comparatione fides exsisteret perfecta. Hac via novimus dies, quibus Eulerus commentationes Academiae nostrae obtulerat, quarum numerus, uti supra jam monuimus, est longe maximus. Reliquas commentationes ordinavimus secundum Actorum ab aliis Academiis editorum annos, aut, si anni non erant indicati, secundum annos, quibus Acta prelo prodierant.

Cl. Jacobius, qui inter viros Germaniae mathematicos incepto nostro singulari favebat studio, ultro in se suscepit laborem diaria Academiae Berolinensis deinceps perscrutandi. Ita huic viro doctissimo multifarias easque gravissimas debemus notitias ad historiam scriptorum ab Eulero compositorum pertinentes. Quae tamen vir ille de vera aetate nonnullarum commentationum arithmeticarum nos docuit, cum ad nos pervenere ipsis Operibus arithmeticis jam sub prelo versantibus, facile explicatur, cur ordo commentationum primo nostro volumine contentarum non prorsus cum vera successione chronologica conveniat, quam non nisi in indice restituere nobis licuit.

(1) Conf. hac de re ipsius Euleri verba in introductione commentationis XC, nunc primum in lucem editae, pag. 576 Tomi II hujus Collectionis, quae sine dubio ipso tractatu de numerorum doctrina posterior est. At omnes hujus rei difficultates ne hodie quidem sublatas esse putamus.

Non opus est monere, in colligenda materia hujus editionis, nos nullo modo solum catalogum *B* ejusque systema secutos esse, quippe qui multis et non levibus scateat erroribus. Si quis libri nostri argumenta cum catalogo illo comparaverit, extemplo reperiet multas commentationes libro nostro inesse, quas catalogus *B* in aliis recensuit disciplinis; alias vero, quas, inscriptionibus minus definitis inducti, in catalogo ad analysin indeterminatam retuleramus, jam a nobis esse omissas.

Cum primi voluminis pars fere dimidia typis expressa esset, collega spectatissimus Bunjakovskius, quem consulueram de adornando indice, cujus auxilio argumenta varia in opere toto exhibita faciliter et sine nimio temporis dispendio evolvi possent, cogitationes exposuit sibi peculiares de systemate aliquo artificiali et datae materiae adaptato, quod potestatem daret loca in opere nostro inveniendi, quae singulae commentationes, imo singula theoremata principalia occupent. Benevole vir doctissimus se periculum facturum pollicitus est talis indicis rationalis conficiendi, modo sibi singulae plagulae traderentur, simulac prelo prodiissent. Conatum hoc, in quo perficiendo doct. Tschebyschevius sedulo ei adfuit, praeter exspectationem, ni fallimur, successit; nec ulli dubitavimus indicem hunc operi nostro subjungere. Quod additamentum lectoribus utilissimum fore confidimus, eosque libenter adstipulaturos esse gratiis, quas hoc loco doctissimis auctoribus obtulisse meum est.

Nomine Miscellaneorum (*Mélanges*), cujus recipiendi necessitas erat, quinque commentationes in hoc indice inveniuntur, quae nullo alio modo in systema quadrare videbantur. Nihilominus jure a nobis receptas esse ratum habemus. Nil vero obstat, quominus parvum hunc commentationum numerum alibi repetamus, si proprium videtur. Ita Legendrius et quadrata magica et problema latrunculi transsilientis ad theoriam numerorum refert. Sed illa quadrata, si respicis imprimis commentationem LXX, una cum tractatibus de numerorum partitione (IX. XXVII), eodem jure ad Analysin combinatoriam referri possunt. Latrunculi vero problema cl. Gaussius summo jure Geometriae situs adscribit. Elucet, singulos tractatus interdum divisioni secundum doctrinas primarias instituendae reluctari, aut saltem dubitationem aliquam de justo loco iis assignando relinquere.

Alterum indicem, cujus auxilio librum possidentes tractatum quemvis, secundum originem citatum, facile evolvant, consulente cl. Jacobio, lubenter confeci atque operi adjunxi, qui et sequentibus operis partibus non deerit.

Idem vir celeberrimus benevole nobis insuper communicavit cogitationes de systemate, secundum quod commentationes in reliquis doctrinis ordinandae sibi viderentur, subjuncta adeo tabula tractatuum omnium, quos singulis partibus adscribendos censet, secundum inscriptiones plerumque, quas catalogus noster *B* offert. Gratus hic labor Geometriam, Analysin universam cum Calculo integrali, Mechanicam et Astronomiam amplectitur. Quod ad disciplinas mere mathematicas attinet, nil obstat, quo minus systema divisionis a cl. Jacobio

propositum omnibus partibus accipiamus, cum non minus simplicitate quam praecisione commendetur. In singulis vero commentationibus secundum systema distribuendis interdum ab amici opinione nobis discedendum fuit, argumentis ipsis accuratius inspectis. Neminem enim fugit inscriptiones commentationum Eulerianarum non omnino valere ad argumenta recte dijudicanda.

Gratum itaque speramus fore iis, qui librum nostrum habebunt, si hoc jam loco conspectum subjungimus proximorum sex voluminum, quibus edendis accingimur. Nam tota materia horum voluminum jamjam collecta et ad opus typographicum disposita est.

Conspectus

sex tomorum subsequentium.

TOMUS III.

Geometria.

Hoc volumen 48 tractatus continebit, qui in prioribus editionibus 1055 paginas implebant. Ineditum adjectum 104 habet paginas manuscriptas.

TOMUS IV.

Analysis algebraica.

Calculus probabilium.

57 commentationes hujus voluminis in prioribus editionibus 1363 paginas implent. Inedita 30 paginas habent manuscriptas.

TOMUS V.

Analysis trigonometrica. Series.

Sunt 58 tractatus, 1217 paginas in prioribus editionibus implentes. Ineditum habet 30 paginas manuscriptas.

TOMUS VI.

Calculi Integralis Pars 1.

54 tractatus 1217 paginis editi. Ineditum 32 paginas habet manuscriptas.

TOMUS VII.

Calculi Integralis Pars 2.

60 tractatus in 1349 paginis editionum priorum.

TOMUS VIII.

Calculi Integralis Pars 3.

73 Tractatus 1412 paginis editi. Inedita habent 55 paginas manuscriptas.

Si opus typographicum eodem deinceps procedet passu ac hucusque, quotannis volumen prodibit singulum. Academia vero etiamnum alit spem, sibi subsidia non defore ad opus editionis maturandum.

Catalogum operum Euleri (*B*), commercio epistolarum a me edito annexum, mancum et interdum vitiosum esse non infitiabor, quippe qui, in laboribus ad editionem omnium operum praeparandam susceptis, hujus imperfectionis multifaria ipse cognovi documenta. Nihilominus idem catalogus solus et optimus pro tempore est fons, ex quo viri docti plenam scriptorum Euleri cognitionem hauriant. Unde nobis persuasum est, operibus etiam mechanicis et astronomicis Euleri eadem cura examinatis, quam in colligendis et ordinandis operibus mere mathematicis impendimus, operae pretium fore, ut catalogum illum omnibus partibus completum et emendatum nova editione publici juris faciamus.

Interim in usum eorum, qui commercium epistolarum illud in manibus habent, additiones nonnullas catalogo adjiciendas hoc loco subjungimus. Census enim operum Euleri editorum *sedecim* commentationibus est augendus, quae et patrem vitam Euleri scribentem et me fugerant, et in utroque catalogo *A* et *B* desunt. Singulas hic enumerabo.

Additamentum catalogi operum Euleri omnium in Commercio epistolarum (Corresp. I. pagg. LI ad CXXI) dati.

1. *Démonstration de la somme de cette série:*

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \frac{1}{36} + \ldots.$$

Vide: *Journal littéraire de l'Allemagne* T. II. part. 1ère p. 115—127. Commentatio haec nomine auctoris caret. Cl. Gaussius, qui humanissime in se susceperat in bibliotheca Göttingensi inquirere, ubinam librorum reperiretur alia quaedam Euleri commentatio (conf. supra p. XVIII), ea occasione in hanc ipsam incidit. Sed cum erroribus scateat typographicis, vir summus non recusavit eam sua manu describere et ad nos in usum editionis transmittere.

2. *Methodus determinandi gradus meridiani pariter ac paralleli Telluris, secundum mensuram a cel.* Maupertuis *cum sociis institutam.* Haec commentatiuncula intexta est tractatui a Winsheimio composito, qui in Comment. vet. T. XII p. 224 reperitur. Id quod cl. Jacobius nobis indicavit.

3. *Meditationes in quaestionem: utrum motus medius Planetarum semper maneat aeque velox, an successu temporis quampiam mutationem patiatur? et quaenam sit ejus causa?* a Carolo Eulero, Leonhardi filio. Praemio donatae A. 1760 (*Recueil des pièces couronnées* etc. VIII). Animi ad hanc commentationem advertendi idem vir clarissimus Jacobius nobis auctor exstitit. Carolus Eulerus, ex filiis Leonhardi secundus, solus fuit, qui nunquam studia mathematica et astronomica coluerit. Medici aulici munere fungens, obiit Petropoli sub finem saeculi. Quantum scio, nullum librum scripsit, ne de medicis quidem tractantem

rebus. Nic. Fussius nobis auctor est Carolum fuisse virum vitae jucunditatibus gaudentem, hilarem, socialem et artem medicam feliciter et fructuose exercentem. Admittamus, quod quidem neutiquam probabile est, eum, tironem in studiis mathematicis et astronomicis, primo illo conatu praemium ab Academia Parisina propositum obtinuisse. Multo tamen minus est verisimile, victorem haec studia prorsus deseruisse. Nulla itaque nobis est haesitatio, cum commentationis tam forma quam materia summus indicetur auctor, quominus etiam hoc opus scriptis Euleri nostri adnumeremus. Quae vero caussa Geometram illum moverit, ut hac occasione verum auctorem nomine celaret ejus filii, quem librum scripsisse nemo confideret, hodie certo enucleare non valemus. Superest tamen suspicio haec: Identidem, non ita pridem, annis nempe 1752, 1753, 1756, 1759, praemia obtinuerat Parisiis, ita ut amici interdum jocati essent Eulerum sibi Academiam Parisinam vectigalem fecisse (vide epistolas Goldbachii pluribus locis). Num ex hac re simulati nominis explicatio est petenda? In sententia fronti commentationis inscripta: «*Ipse Pater statuit quaenam coeli astra moveret*», filii, cujus nomen pater mutuatus erat, facetiam insignem libenter agnoscimus.

4. *Dissertation sur la meilleure construction du Cabestan. Cette pièce est une des quatre, entre lesquelles le prix double* (de 1741) *a été partagé.* (Recueil des pièces couronnées T. V p. 29—87.)

5. *Meditationes in quaestionem ab Ill. Academia regia Parisina scientiarum, pro anno* 1747 *cum praemio duplicato propositam: Quibusnam observationibus mari, tam interdiu quam noctu, itemque durante crepusculo, verum temporis momentum commodissime et certissime determinari queat?* (Recueil d. p. cour. T. VI. p. 111—167.) In epistolis (*Corresp.* I p. 608) legimus has duas commentationes praemio ornatas fuisse. Utraque, ut vidimus, in collectionem: *Recueil des p. cour.* recepta est, sed sine auctoris nomine indicato. Archetypum N. 4 latine conscriptum, de quo supra retulimus, omne de origine tollit dubium. Ambigitur id tantum, utrum Eulerus ipse tractatum gallice scripserit, an versio Parisiis sit facta. Quod jam ad N. 5 attinet, Daniel Bernoullius m. Aprili a. 1747 (*Corresp.* II p. 619) scribit, praemium duplex inter se et alium divisum esse, quem Eulerum fuisse Parisiis judicetur. Ex quatuor commentationibus vero, quae in tomo VI collectionis illius ante citatae tractatum Bernoullianum sequuntur, sola Euleriana potest esse prima illa, cui sententia praeest: *Arbor non uno sternitur ictu.* Ita rem vere se habere, lectio operis unumquemque docebit [1].

(1) Lectorum judicio relinquimus, nonne haec occultatio nominis, jam post approbationem publicam, singulare sit modestiae documentum, ex eodem fortasse momento explicandum, ac prior mutuatio nominis a filio? In Epistolis (*Corresp.* I p. 145) de alia adhuc commentatione sermo est, *de motu fluidorum in canalibus elasticis* tractante, quam Eulerus m. Martio a. 1742 ad Academiam Divionensem pro obtinendo praemio ab ea proposito miserat, nullo, quod dolendum est, retento apographo. Cum haec commentatio nobis prorsus ignota sit, operae non indignum nobis visum est de ejus sorte percontari; sed ad literas nostras m Nov. huj. anni Divionem missas responsio nobis nondum pervenit.

Messem exspectatione uberiorem Acta Eruditorum Lipsiensia denuo examinata nobis tulerunt. Ex septem commentationibus infra citatis a N. 6 ad N. 12, duas ipse detexi, reliquas quinque indicatas debeo doctissimo collegae Petersio.

6. A. 1726 p. 361. *Constructio linearum isochronarum in medio quocunque resistente.* Haec commentatiuncula peculiaris est momenti, cum hoc sit primum specimen ab Eulero publici juris factum. Antehac ambigebatur, utra fuerit commentatio primum edita, num N. 500 catal. *B*: *Dissertatio physica de sono*, Basileae 1727, qua cathedram physices in Universitate patria petebat; an altera *B*, N. 601, quae, Parisiis 1727 praemio ornata, de malis in navibus erigendis (*de malorum implantatione*) tractat.

7. A. 1727 p. 408. *Methodus inveniendi trajectorias reciprocas algebraicas.*

8. A. 1746 p. 92. *Animadversio ad libri «Methodus inveniendi lineas curvas maximi minimive proprietate gaudentes» paragraphum* 83. Tractatus ille: *Methodus inveniendi* cet. ad D. Bernoullium autographus missus erat, qui traderetur bibliopolae Bousquetio, viro de edendis operibus mathematicis Lausannae tum temporis egregie merito. Bernoullius, perlecto opere, Eulero animadversiones nonnullas misit de problemate curvae elasticae. Cum vero opus sub prelo esset, emendationum nullus erat locus in ipso opere faciendarum, quas haec nostra exhibet commentatio.

9. A. 1746 p. 230. *Solutio problematis catoptrici in Novis Actis Erudilor. A.* 1745 *mense Sept. p.* 523 *propositi* et

10. A. 1748 pagg. 27. 61. 169. Tractatus eodem modo inscriptus. Prior harum commentationum finem solutionis summatim exponit, quam invenit Eulerus problematis a se ipso a. 1745 propositi. N. 10 vero elegantissimam ejus exhibet analysin. Vide supra adnotationem in N. 15 Ineditorum datam. Altera solutionis forma eaque prorsus diversa, ex anno 1745, est in epistolis *Corresp.* I p. 341—354.

11. A. 1747 p. 267. *De numeris amicabilibus.* Haec commentatiuncula $2\frac{1}{2}$ tantum paginas implens, primo adspectu, mera relatio visa est de magno tractatu X (Vide collectionis nostrae T. I pag. 102 ad 145). Attamen in recensu huic relationi annexo, qui 30 exhibet paria numerorum amicabilium, quatuor eorum reperiuntur, qui desunt in catalogo tractatus majoris, 61 paria talium numerorum offerente. Haec quatuor numerorum amicabilium paria sunt insuper ex simplicioribus. Quae res nos movit, ut brevem hanc relationem, una cum excerptis ex N. 56 Ineditorum, in fine tomi nostri II appendicis loco adjiceremus.

12. A. 1749 p. 512. *De vibratione chordarum exercitatio.* Est archetypum latine conscriptum illius versionis gallicae, quae tomo IV Actor. Berolinens. 1748 p. 69 prelo impressa reperitur et in catal. nostro *B*. N. 520 prae se fert.

13. *Extract of a letter from M.* Leonard Euler *etc. to the Rev. M.* Ch. Wetstein, *Chaplain and Secretary to* H. R. H. *the* Prince of Wales, *concerning the discoveries of*

the Russians on the Nord-East Coast of Asia d. d. Berlin 1746 *Dec.* 10 (*Philos. Transact. f.* 1747 *p.* 421).

14. *Extract of a letter from Prof.* Euler *of Berlin to the Rev. M.* C. Wetstein (*Philos. Transact. f.* 1751. 1752. *p.* 263). De problemate ab Academia Petropolitana proposito: Num theoria Newtoniana ad omnes motus lunaris irregularitates explicandas valeat?

15. Epistola ad Shortium missa, adjuncta alia Dollondio tradenda, qua reprehensiones contra objectiva Euleriana prolatas refutat (*Philos. Transact. f.* 1753 *p.* 292).

16. Denique liber periodicus, qui a Cl. Crellio editur (*Journal für reine und angewandte Mathematik* T. XXXV p. 106) opusculum hucusque ineditum obtulit: *Commentatio de Matheseos sublimioris utilitate*, quod typis excusum est secundum autographum in collectione Dr. Friedländeri Berolini servatum.

Ex supra allatis sequitur commentationem, quae, auctoritate catalogi A, in nostrum migraverat catalogum B, ubi est N. 3, delendam esse, cum nulla talis commentatio inter editas exstet; deinde NN. 41 et 74 catalogi B, cum duae sint editiones ejusdem commentationis, sub uno numero jungi debere, altero sublato. Pariter tractatus N. 12 enumerationis praecedentis, non nisi lingua diversus a N. 520, novum catalogi numerum constituere nequit. Praeterea denique duae commentationes in catalogo B binis occurrunt locis, ita ut altero loco deleri debeant, quae sunt

N. 198 = N. 429, N. 321 = N. 324.

Ita nunc, computo facto generali, summa omnium Euleri scriptorum, majorum et minorum, editorum et ineditorum, evadit = 808.

Quamquam opus hoc a nobis editum, Arithmetica Euleriana complectens, suis finibus integrum est, multo magis tamen arridet, duas ipsius partes pro initio haberi majoris collectionis, multa volumina amplexurae. Talis vero magna collectio narratione de vita illustris Euleri nullo modo carere debet. Quae res nos impulit, ut operi huic nostro Euleri *laudationem* a N. Fussio conscriptam adjunxerimus, in qua nil mutare nobis religio fuit, nisi lapsus aliquos calami. Hoc patris nostri opusculum, si dictione et ornatu inferius videri potest libro saepius typis repetito, quem Condorcetius in memoriam Euleri legit et edidit, ita tamen praestat, sine dubio, et calore verborum et summa rerum narratarum veritate et judicio solidiori de Euleri doctrina et scriptis lato. Hanc esse sententiam etiam aliorum virorum doctorum, nos filii narratoris confidimus.

Petropoli, m. Decembri 1848.

P. H. Fuss.

ELOGE

DE

LÉONARD EULER

LU A L'ACADÉMIE IMPÉRIALE DES SCIENCES DE St.-PÉTERSBOURG,

le 23 Octobre 1783,

par

NICOLAS FUSS.

Représenter le cours de la vie d'un grand homme qui a illustré son siècle en éclairant le monde, c'est faire l'éloge de l'esprit humain. Celui qui se charge de l'exécution de cet intéressant tableau, s'efforcera envain de remplir dignement sa tâche, s'il ne joint à une connaissance parfaite des sciences dont il doit montrer les progrès, tous les agréments du style que le genre panégyrique exige, et qu'on dit être incompatibles avec l'étude des sciences abstraites. Quoique dispensé, d'un côté, du soin d'embellir son sujet, assez grand par lui-même, le Biographe, en s'attachant aux faits, ne saurait se soustraire à l'obligation de les arranger avec goût, de les présenter avec clarté et de les peindre avec force. Il doit montrer comment la Nature fait naître un grand homme; il doit démêler les circonstances qui viennent à l'appui de son développement; et en exposant, par le détail des travaux littéraires du savant dont il trace l'éloge, ce qu'il a fait pour les sciences, il ne doit pas oublier d'examiner l'état où elles étaient avant cette époque, et fixer de cette façon le point d'où il est parti.

En me chargeant de présenter à cette assemblée le tableau de la vie de l'immortel Euler, j'ai senti toutes ces obligations, et j'ai vu qu'il me sera d'autant plus difficile de les remplir dignement, qu'outre le sentiment profond de mon incapacité, augmenté par la douleur que la mort de M. Euler m'a causée, et que je sens renaître en ce moment, les bornes étroites d'un discours académique ne me permettront pas de m'acquitter de tous les devoirs d'un biographe. Je ne donnerai donc qu'une légère ébauche de la vie de ce grand homme; et en fournissant des matériaux à celui qui se sentira assez de forces pour faire un panégyrique digne de lui, je me contenterai d'avoir jeté quelques fleurs sur la tombe de mon cher et illustre Maître.

Léonard Euler, Professeur de Mathématiques, Membre de l'Académie Impériale des Sciences de St.-Pétersbourg, ancien Directeur de l'Académie Royale des Sciences et Belles-Lettres de Prusse, Associé étranger de l'Académie Royale des Sciences de Paris, de la Société Royale de Londres, etc. naquit à Bâle, le $^{4}/_{15}$ Avril 1707, de Paul Euler, alors Pasteur désigné de Riehen, et de Marguerite Brucker, issue d'une famille favorablement connue dans la république des lettres, par plusieurs savants distingués qui ont porté ce nom.

Il passa les premières années de son enfance à Riehen, et c'est à ce séjour champêtre, dans un pays où les progrès de la corruption ont toujours été lents, joint à l'exemple de ses parents, qu'il a dû probablement cette simplicité de caractère et cette pureté de moeurs, digne du premier âge, qui l'ont distingué toute sa vie, et qui ont probablement contribué à le mettre en état de fournir la carrière longue et brillante qui a immortalisé son nom.

Aux premières instructions que son père eut soin de lui donner, il joignit les mathématiques, qu'il aimait et qu'il avait étudiées lui-même avec succès sous le célèbre Jacques Bernoulli. Destinant son fils à l'état ecclésiastique, il ne se doutait pas que ce qui d'abord ne devait être qu'un amusement instructif, deviendrait, dans la suite, l'objet de l'application la plus sérieuse et la plus opiniâtre. Mais le germe qu'il avait mis dans l'ame du jeune Géomètre ne tarda pas à pousser de profondes racines. Quoique trop bien organisé pour montrer un talent exclusif pour les sciences mathématiques, ce n'était qu'en s'y livrant tout entier que son génie se sentait dans son élément.

Heureusement, son père ne pensa pas encore à le détourner d'une étude qu'il aimait trop lui-même, dont il sentait trop bien l'influence sur le développement de la faculté de penser, et l'utilité dans toutes les branches de nos connaissances, pour la lui défendre sérieusement. Le génie du jeune Euler eut tout le temps de se développer, et il le fit avec cette rapidité qui annonce toujours les talents supérieurs et qui fut le présage de sa grandeur future.

Envoyé à Bâle pour y faire son cours de philosophie, M. Euler fréquenta régulièrement les leçons des professeurs de l'Université. Sa mémoire prodigieuse le mit en état de passer rapidement sur tout ce qui n'était pas géométrie, et de consacrer à cette science favorite tout le reste de son temps. Avec un penchant si marqué pour les mathématiques, et un esprit enflammé que de grands progrès ne rendaient que plus avide d'instruction, il ne tarda pas à être connu de Jean Bernoulli, le plus grand des géomètres alors vivants. Celui-ci le distingua bientôt de ses autres auditeurs, et ne pouvant se rendre aux instances que le jeune mathématicien lui faisait, de lui accorder des leçons particulières, il s'offrit à lui lever, tous les samedis, les difficultés qu'il aurait rencontrées en étudiant les ouvrages les plus difficiles. Méthode excellente! mais qui ne peut réussir qu'avec un génie aussi ardent, accompagné d'une assiduité aussi infatigable que l'était celle de M. Euler, destiné dès-lors à surpasser un maître qui avait fait époque dans l'histoire des mathématiques.

Ayant reçu, en 1723, le grade de maître-ès-arts, après avoir prononcé un discours en latin, sur la philosophie de Newton comparée avec celle de Descartes, M. Euler embrassa, pour se conformer aux volontés de son père, l'étude de la théologie et des langues orientales. Cette étude que sa destination rendait nécessaire, quoique peu analogue à son génie, ne fut pas sans succès; mais bientôt, rendu par le consentement de son père à la géométrie, dont rien n'avait pu le détacher entièrement, il s'y précipita avec une ardeur redoublée. Il continua à consulter M. Bernoulli, et lia une amitié étroite avec ses deux fils Nicolas et Daniel. C'est cette liaison, fondée sur la conformité des penchants, qui a procuré à l'Académie l'avantage de le posséder.

Cathérine I venait d'exécuter un projet que Pierre-le-Grand avait formé, celui d'ériger dans sa capitale une Académie des sciences. Les deux jeunes Bernoulli y furent appelés en 1725, et à leur départ ils promirent à M. Euler, qui désira ardemment de les y suivre, qu'ils feraient leur possible pour lui trouver une place convenable. En lui écrivant l'année suivante qu'ils avaient trouvé ce qu'ils cherchaient, ils lui conseillèrent en même temps d'appliquer ses connaissances mathématiques à la physiologie.

Un grand talent ne peut jamais se démentir. Pour devenir Physiologue, M. Euler n'eut qu'à le vouloir. Il se fit mettre sur la liste des étudiants en médecine et fréquenta, avec l'ardeur d'un génie impatient d'entrer dans une carrière brillante, les leçons des plus habiles médecins de Bâle.

Cette étude, loin de tendre tous les ressorts de son esprit aussi actif que vaste, lui laissa assez de loisir pour composer, dans le même temps, une dissertation sur la nature et la propagation du son, et une réponse à la question sur la mâture des vaisseaux, que l'Académie de Paris jugea digne de l'accessit, en 1727. Cet écrit et une des thèses

qu'il défendit pour obtenir la chaire de physique vacante à Bâle, font voir que M. Euler a tourné de bonne heure ses vues du côté de la navigation, qu'il a enrichie, dans la suite, de tant de nouvelles découvertes.

Heureusement, pour notre Académie, le sort, qui décide à Bâle des places, tant dans la Magistrature que dans l'Université, lui fut contraire, et peu de jours après ce contre-temps, il quitta sa patrie pour se rendre à St.-Pétersbourg, où il trouva un théâtre plus digne du rôle éminent qu'il devait jouer dans la république des lettres. Son début répondit à l'attente que l'Académie et ses compatriotes, Hermann et Daniel Bernoulli, s'étaient faite de lui.

Déclaré adjoint pour les mathématiques, sans qu'il fut plus question de physiologie, il se voua par état à une étude, à laquelle ni les intentions de son père, ni le peu de fortune qu'elle offre ordinairement, n'avaient pu le faire renoncer. Il enrichit d'abord les premiers volumes des Commentaires de plusieurs mémoires, d'un prix à exciter une noble émulation entre lui et M. Daniel Bernoulli, émulation qui a duré toujours, sans altérer leur amitié et sans dégénérer en jalousie; sentiment indigne d'une ame généreuse, et qui ternit l'éclat des plus belles vertus.

La carrière des mathématiques, dans le temps où M. Euler y entra, n'était rien moins qu'encourageante. Un talent médiocre ne pouvait guère espérer de s'y faire un nom: il fallait ne pas y entrer, ou s'y distinguer d'une manière brillante. La mémoire des grands hommes qui avaient illustré la fin du siècle passé et le commencement du nôtre, était dans sa première vigueur: A peine Newton et Leibnitz, qui avaient fait changer de face la géométrie, étaient-ils morts; l'on n'avait pas encore perdu le souvenir des importants services que les découvertes de Huyghens, Bernoulli, Moivre,. Tschirnhausen, Taylor, Fermat, et de tant d'autres géomètres, avaient rendus à toutes les branches des sciences mathématiques.

Après cette époque brillante que restait-il à M. Euler? Pouvait-il espérer que la nature, qui n'est pas prodigue de ses dons, fit encore un miracle en sa faveur, après avoir organisé tant de têtes mathématiques à la fois? Il sentit ce qu'elle avait fait pour lui; il entra dans la carrière avec cette noble assurance que le sentiment d'une supériorité décidée inspire, et il fit voir que ses prédécesseurs n'avaient pas épuisé tous les trésors de la géométrie et de l'analyse.

Effectivement, le calcul infinitésimal était encore trop près de son enfance, pour qu'à peine sorti des mains de ses créateurs, il eût pu avoir atteint un degré considérable de perfection. La mécanique, la dynamique, et surtout l'hydrodynamique et la science du mouvement des corps célestes, se ressentaient de l'imperfection de ce nouveau calcul: on avait assez bien appris à y appliquer le calcul différentiel; mais on rencontrait partout des difficultés, dès qu'il s'agissait de remonter des éléments aux grandeurs mêmes. Pour ce qui regarde la connaissance de la nature et des propriétés des nombres, les écrits de Fermat, qui y avait travaillé avec tant de succès, étaient perdus, et avec eux toutes ses profondes recherches. L'artillerie et la navigation étaient réduites à des principes vagues et fondés sur un tas d'observations, souvent contradictoires, plutôt que sur une théorie suivie. Les irrégularités dans les mouvements des corps célestes et surtout la complication des forces qui influent sur celui de la lune, n'avaient cessé de désespérer tous les géomètres. L'astronomie pratique luttait encore contre les imperfections des télescopes: à peine peut-on dire qu'il existât des règles pour leur construction. M. Euler tourna successivement ses vues sur tous ces différents objets; il perfectionna le calcul intégral; il fut l'inventeur d'un nouveau genre de calcul, celui des sinus; il simplifia les opérations analytiques; et à l'aide de ces puissants secours, et de l'étonnante facilité avec laquelle il sut manier les expressions les plus intraitables, il parvint à répandre un nouveau jour sur toutes les parties des sciences mathématiques.

Peu de temps après sa réception à l'Académie, M. Euler fut sur le point d'embrasser un état bien différent de celui que son penchant lui avait fait choisir. La mort de l'Impératrice Cathérine I menaça de l'anéantissement un institut qui était trop nouveau pour avoir pris de la consistance. On ne vit qu'avec indifférence une Académie qui coûtait annuellement des sommes considérables, sans être d'une utilité palpable. On ne connaissait pas encore le véritable point de vue, d'où il faut envisager les sociétés littéraires, destinées à rassembler toutes les découvertes utiles, à les répandre et à les perfectionner. Les académiciens sentirent la nécessité de prendre leurs mesures en

conséquence, et M. Euler se décida à entrer dans la marine. L'amiral de Sievers, à qui un homme comme Euler parut être une trouvaille pour la marine naissante, lui offrit une lieutenance de vaisseau, en lui promettant un prompt avancement.

Heureusement, les circonstances changèrent en faveur de l'Académie, et lorsqu'en 1730, MM. Hermann et Bülffinger la quittèrent pour retourner dans leur patrie, on conféra à M. Euler la place de professeur de physique, qu'il remplit jusqu'au départ de son ami Daniel Bernoulli, dont il fut nommé le successeur, en 1733.

Le grand nombre des mémoires que M. Euler avait présentés à l'Académie jusqu'à cette époque, font foi de sa fécondité surprenante, de sa grande facilité à traiter les questions les plus difficiles, et de son extrême application. Il en fournit un exemple bien plus frappant, lorsqu'il s'agissait, en 1735, de faire un calcul qui exigeait de la hâte, et pour lequel les autres mathématiciens avaient demandé quelques mois de temps. M. Euler s'engagea à le faire en trois jours; et il le fit au grand étonnement de l'Académie. Mais que ce travail lui coûta cher! il lui attira une fièvre chaude qui le mit au bord du tombeau. Il en revint pourtant, mais avec la perte de l'oeil droit que lui ravit un abcès survenu pendant la maladie. La perte d'un organe aussi précieux eût été pour tout autre un puissant motif de se ménager, afin de conserver l'oeil qui lui restait, mais il ne connut point de relâche; il eût renoncé aussi facilement à la nourriture qu'au travail, dont l'habitude perpétuelle lui avait fait un besoin.

La grande révolution que la découverte du calcul différentiel et du calcul intégral avait opérée dans presque toutes les branches des sciences mathématiques, ne laissa pas de faire changer aussi entièrement de face la mécanique. Newton, Bernoulli, Hermann, et Euler lui-même, avaient enrichi successivement cette partie sublime et nécessaire des mathématiques mixtes d'une infinité de nouvelles découvertes. Cependant il n'existait point d'ouvrage complet sur la science du mouvement, à l'exception de deux ou trois, dont M. Euler sentait toute l'insuffisance. Il voyait avec peine que les Principes de la philosophie de Newton et la Phoronomie de Hermann, c'est-à-dire ce qu'il y avait de mieux sur cette matière, cachassent, sous le voile de la synthèse, la route, par laquelle ces grands hommes étaient parvenus à enrichir la mécanique de tant d'importantes découvertes. Il employa, pour la déterrer, toutes les ressources de l'analyse, qu'il avait si bien en son pouvoir, et qui l'avait mis en état de résoudre tant de questions que personne avant lui n'avait osé aborder: Il lia ses découvertes à celles des autres géomètres, les rédigea dans un ordre systématique, et l'Académie les fit imprimer en 1736.

La clarté dans les idées, la précision dans leur énoncé, l'ordre dans leur arrangement, sont des qualités essentielles que tout auteur, qui veut devenir classique, doit tâcher de donner à ses ouvrages: elles font le moindre mérite de la Mécanique de M. Euler. L'obscurité et le désordre ne sont pas des défauts qu'on reprochera jamais à celui qui a su répandre la lumière et la clarté sur ses plus profondes recherches. Cet ouvrage fixa la renommée de M. Euler et lui assigna une place parmi les premiers géomètres vivants. Et c'est beaucoup dire, si l'on considère que Jean Bernoulli vivait encore. A peine entré dans la carrière, il n'est donné qu'au génie supérieur de s'élancer d'un pas aussi rapide et de se placer à côté d'un homme couvert de la gloire de tant de victoires, remportées sur tous les géomètres anglais et français qui avaient osé se mesurer avec lui.

J'ai déjà remarqué que M. Euler, dès son entrée à l'Académie, avait enrichi les Commentaires d'une quantité de mémoires qui portent tous l'empreinte du génie. C'est là qu'on trouve épuisée la théorie des courbes les plus remarquables les Tautochrones, les Brachystochrones, les Trajectoires, etc. les plus profondes recherches sur le calcul intégral, sur la nature des nombres, sur les séries, sur le mouvement des corps célestes, sur l'attraction des corps sphéroïdico-elliptiques, et sur une infinité d'objets, dont la centième partie suffirait pour faire la renommée d'un autre que lui. Mais ce qui dut accomplir sa gloire et faire reconnaître sa supériorite dans l'analyse, c'est la solution du problème des isopérimètres, si fameux par la controverse entre les deux frères Jacques et Jean Bernoulli dont chacun prétendait en avoir trouvé la solution et qu'aucun n'avait connu dans toute son étendue. Le nombre et le prix

de tous ces mémoires étonne, et on ne conçoit pas, comment un seul homme a pu suffire à tant de travaux, dont le détail seul nous effraie.

On sent bien qu'un homme aussi laborieux n'a guère pu prendre part aux dissipations où les liaisons, qu'une grande réputation fait naitre, peuvent entrainer un homme admiré, et qu'on aurait pardonnées à son âge et à son tempérament naturellement gai et sociable. Un des principaux délassements que M. Euler se permettait, c'était la musique, et même il ne s'y abandonnait qu'accompagné de son esprit géométrique. En se livrant aux sensations agréables de l'harmonie, il en approfondissait la cause, et au milieu de ses accords, il en calculait les proportions. On peut dire que c'est pour son délassement, et dans les moments de repos que son esprit cherchait pour se recueillir, qu'il composa son essai d'une nouvelle théorie de la musique, publié en 1739. Ouvrage profond et rempli d'idées neuves, ou présentées sous un nouveau point de vue; mais qui n'eut pas un grand succès, apparemment par la seule raison qu'il renferme trop de géométrie pour le musicien, et trop de musique pour le géomètre. Cependant il contient, indépendamment de la théorie, bâtie en partie sur les premiers fondements jetés par Pythagore, quantité de choses dont le compositeur et le faiseur d'instruments de musique pourraient tirer un grand parti; et d'ailleurs, la doctrine des genres et des modes de musique y est traitée et présentée avec la clarté et la précision qui caractérisent tous les ouvrages de M. Euler.

Pour ce qui regarde la théorie même, dont la partie physique est au-dessus de toute contestation, M. Euler, en cherchant la source du plaisir de l'harmonie, part de ce principe: que la perception d'une perfection quelconque fait naitre le sentiment du plaisir; et que, comme l'ordre est une des perfections qui causent à l'ame des sensations agréables, tout le plaisir que nous fait goûter une belle musique, consiste dans la perception des rapports que les sons tiennent entre eux, tant relativement à la durée dans leur succession, que par rapport à la fréquence des vibrations de l'air qui les produisent. C'est sur ce principe métaphysique, modifié et appliqué à toutes les parties de la musique, que le système de M. Euler est appuyé.

On a taxé ce principe d'insuffisance; et comme il n'est pas dans le pouvoir du géomètre, de soumettre les qualités relatives de notre ame à la rigueur de ses calculs, il est difficile d'en démontrer la solidité; mais ce principe accordé, on sera obligé de convenir qu'il est impossible d'en faire un meilleur usage, ni de raisonner avec plus de subtilité et de pénétration. D'ailleurs, toutes les objections contre ce principe, fussent-elles insolubles, ne feraient que peu de tort à l'ouvrage même. Il serait semblable à un édifice parfait dans toutes ses parties, mais bâti sur un terrain mouvant: en admirant l'habileté de l'architecte, on le plaindrait de n'avoir pu le construire sur un fond plus solide.

Avant la publication de ce traité sur la musique, M. Euler avait déjà mis au jour un traité d'arithmétique. Plusieurs académiciens s'étaient chargés, sur la demande de leur chef, de composer des ouvrages élémentaires, et notre géomètre ne crut point s'abaisser par un travail, inférieur à ses forces, mais anobli par son but, qui était l'instruction publique. La complaisance, avec laquelle il se prêtait à toutes les commissions extraordinaires, et le zèle qu'il mettait dans leur exécution, lui en attira plusieurs, et entre autres l'inspection du département géographique, que le Sénat dirigeant lui conféra en 1740.

M. Euler avait vu naitre une nouvelle occasion de déployer toutes les forces de son génie, lorsque l'Académie de Paris, qui avait déjà couronné, en 1738, son mémoire physique sur la nature et les propriétés du feu, proposa, pour 1740, la question du flux et du reflux de la mer; question importante, mais dont la solution exigeait des calculs effrayants et un système entier du monde. Sa pièce sur ce sujet, couronnée en 1740, est un chef-d'oeuvre d'analyse et de géométrie. Il n'eut pas, à la vérité, le prix entier; mais D. Bernoulli et Mac-Laurin n'étaient pas des rivaux indignes d'avoir part à son triomphe. L'Académie n'a pas vu souvent une concurrence aussi brillante, et peut-être a-t-elle reçu sur peu de questions trois mémoires du prix de ceux que je viens de nommer. Celui de M. Euler est surtout remarquable par la clarté, avec laquelle il explique les effets que l'action du soleil et de la lune,

à l'exclusion de toute autre force, exercent sur la mer; par la belle détermination de la figure de la terre, en tant qu'elle est changée par l'action de ces deux forces; par la pénétration avec laquelle, en regardant les mouvements de la mer comme oscillatoires, il supplée aux effets de l'inertie des eaux, qu'il avait été obligé de supposer nulle au commencement; par les intégrations heureuses que la considération de ce mouvement réciproque exigeait, et par la sagacité enfin dans l'explication des principaux phénomènes de la marée selon sa théorie.

Si quelque chose peut contribuer à augmenter la confiance qu'on doit avoir aux sublimes recherches de M. Euler sur ce sujet, après les avoir trouvées si conformes à l'expérience, c'est, sans contredit, le merveilleux accord qui se trouve entre son mémoire et celui de M. Bernoulli. Partis de principes assez différens, l'un adoptant, par exemple, l'hypothèse des tourbillons que l'autre rejette, ils arrivent au même but; ils se sont même rencontrés en plusieurs endroits, comme entre autres dans la détermination de la marée sous la zone glaciale. C'est ainsi que la vérité paraît se multiplier quelquefois, pour se communiquer à ses vrais confidens, par quelque route qu'ils aillent la chercher.

J'ai remarqué en général que M. Euler s'est souvent rencontré avec d'autres géomètres, et particulièrement avec M. Bernoulli, dans les recherches de mathématiques mixtes. M. Bernoulli a eu quelquefois sur lui l'avantage d'une plus grande précision dans les principes physiques. Il avait la patience de se faciliter les suppositions que ses calculs exigeaient, par des expériences faites avec beaucoup de jugement et d'adresse. M. Euler, que l'ardeur du travail entraînait, n'en a fait que rarement. Sûr de son instinct naturel à sentir le faux et le vrai, et de son adresse à estimer, d'après des combinaisons et des analogies, ses hypothèses étaient quelquefois trop hardies, mais sa supériorité dans l'analyse le mettait toujours au-dessus de M. Bernoulli et de tout autre, dès qu'il s'agissait de simplifier les expressions, de les adapter à la pratique, et de reconnaître, par les formules finales, la nature du résultat.

Il y a des savans qui doivent leur réputation à leur correspondance; il y en a d'autres qui doivent l'avantage d'une grande correspondance, si c'en est un, à leur réputation: celle de M. Euler ne manqua pas de lui attirer des lettres de toutes parts. Tout ce qu'il y avait de plus illustre parmi les géomètres des nations les plus éclairées, s'empressa d'entrer en correspondance avec lui. Le commerce de lettres qu'il entretint avec Jean Bernoulli, avait commencé dès 1727; et le Nestor de la géométrie ne crut point s'abaisser, en demandant bien des fois les avis de son ancien disciple, et en soumettant ses travaux à son jugement. (1)

Nous arrivons à une époque remarquable de la vie de M. Euler. La multiplicité et les brillans succès de ses travaux, qui avaient répandu son nom par toute l'Europe, lui attirèrent en 1741 des propositions de la part du ministre de Prusse, comte de Mardefeld. L'ancienne Société royale, fondée par Leibnitz, paraissait reprendre de nouvelles forces, par les soins que Frédéric II lui donna dès son avènement au trône. Il avait déjà conçu le projet digne de lui, d'ériger une académie des sciences, en refondant l'ancien établissement, et c'est pour cette raison qu'il appela M. Euler à son service. L'état chancelant de notre Académie sous la régence, rendait encore plus acceptables des propositions très avantageuses en elles-mêmes. M. Euler se rendit donc aux invitations du Roi et quitta Pétersbourg avec sa famille au mois de Juin 1741, pour donner de l'éclat à une académie, qui allait naître sous les auspices d'un philosophe couronné.

(1) Pour donner une idée du ton qui régnait dans les lettres de ces deux hommes illustres, et du grand cas que M. Bernoulli a fait de bonne-heure du génie de M. Euler, il suffit de donner ici la fin d'une de ses lettres, prise au hasard parmi celles de 1739:

«De caetero gratissimum mihi fuit intelligere, quod ad admirationem usque Tibi placuerint quae scripsi de oscillationibus verticalibus, propter simplicitatem expressionis et insignem usum, quem praestare possunt in explicandis navium ponderibus; maluissem autem, ut ipse quoque calculum fecisses ex Tuo ingenio, quo mihi patuisset annon in ratiocinando erraverim. Nam ingenue fateor, me Tuis luminibus plus fidere quam meis. Quae uberius affers, Vir excell de Isoperimetricis, credo equidem Te omnia probe ruminasse atque ad veritatis trutinam expendisse, ita ut vix quicquam restet, quod acerrimam Tuam sagacitatem subterfugere potuerit: etc.»

Arrivé à Berlin, il eut d'abord lieu d'être flatté des attentions du Roi, qui lui écrivit du camp de Reichenbach, du milieu de ses occupations guerrières. Mais il trouva l'ancienne Société presque expirante. La guerre, toujours funeste aux sciences, avait retardé les intentions gracieuses du Roi. Cependant il s'était formé une nouvelle société littéraire, composée en partie des membres de la Société royale et en partie d'autres hommes de lettres. M. Euler en fut membre et décora le dernier volume des Mélanges de Berlin de cinq mémoires qui sont peut-être ce qu'il y a de mieux dans cette collection. Il leur fit succéder, avec une rapidité étonnante, ce grand nombre de recherches éparses dans les Mémoires dont l'Académie, dès son établissement en 1744, a eu soin de publier régulièrement un volume par an.

Cette quantité prodigieuse de mémoires, sur tout ce qu'il y a de plus profond dans les mathématiques, toujours remplis de vues neuves, souvent de vérités sublimes, et quelquefois des plus importantes découvertes, doit nous étonner d'autant plus, que M. Euler ne discontinuait point d'en fournir aussi régulièrement à l'Académie de St.-Pétersbourg, qui lui accorda, dès 1742, une pension, et dont les Commentaires sont remplis à moitié des fruits de son étonnante fécondité. A voir ses productions se succéder si rapidement, on eût dit que les calculs les plus laborieux, les plus sublimes méditations ne lui coûtaient rien que de les écrire. Et la postérité aura de la peine à croire que la vie d'un homme ait pu suffire aux travaux dont on verra la liste à la suite de cet éloge[1].

En traitant le problème important des isopérimètres, M. Euler avait déjà reconnu la grande utilité de cette recherche tant dans l'analyse pure que dans la solution des problèmes de physique. Il avait remarqué que toutes les lignes courbes que ces sortes de problèmes fournissent, sont douées d'une espèce de *plus-grand* ou de *plus-petit*, et qu'on en peut trouver plusieurs par la seule méthode des isopérimètres. Il alla même jusqu'à avancer, que tous les effets quelconques pourraient être déterminés par la méthode des plus-grands et des plus-petits, c'est-à-dire, par les causes efficientes, pourvu qu'on pût toujours entrevoir le maximum ou le minimum que la nature affecte. M. Daniel Bernoulli s'était servi de cette voie pour déterminer la figure d'une lame élastique courbée, sans reconnaître pourtant l'équation générale de la courbe élastique dans son équation, n'en ayant pas su poursuivre le développement; il l'écrivit à M. Euler, avec la conjecture, que les trajectoires décrites autour d'un ou de plusieurs centres de forces pourraient être déterminées par la même méthode. M. Euler reprit ce sujet important, et il mit au jour, en 1744, un traité complet des isopérimètres, où l'on peut dire qu'il a prodigué toutes les richesses de la plus sublime analyse, et où il a jeté les premiers fondemens du calcul des variations, en considérant des courbes qui diffèrent infiniment peu d'une courbe proposée.

La même année, qui fut aussi l'époque du renouvellement de l'Académie, et celle de sa nomination à la place de directeur de la classe mathématique, M. Euler publia sa Théorie du mouvement des planètes et des comètes; sujet qu'il a encore enrichi, dans la suite, d'une infinité de nouvelles découvertes.

La Théorie de l'aimant, qui remporta le prix de l'Académie de Paris en 1744, est trop connue, pour qu'il soit besoin d'en parler beaucoup. En partant de l'idée heureuse de Descartes, que tous les phénomènes de l'aimant proviennent de la circulation d'un fluide subtil par les conduits imperceptibles des corps magnétiques, M. Euler se figure les pores de l'aimant sous la forme de tuyaux contigus, parallèles, hérissés, comme les veines, de valvules, et si étroits qu'ils ne laissent passer que la partie la plus subtile de l'éther, dont l'élasticité pousse cette partie plus déliée dans les pores de l'aimant, et la force à se replier à sa sortie, pour y rentrer de nouveau, et former ainsi une espèce de tourbillon. Par cette idée ingénieuse, développée avec beaucoup de sagacité, M. Euler est en état d'expliquer tous les phénomènes du magnétisme; et l'accord de l'expérience avec cette hypothèse, si conforme aux lois générales de la nature, parle en faveur de sa probabilité.

La même année, le Roi demanda l'avis de M. Euler sur le meilleur traité d'artillerie. Il avait paru en Angleterre un ouvrage sur les principes d'artillerie, dont l'auteur était ce même Robins qui avait attaqué M. Euler dans une

(1) Nous ne la reproduisons pas, renvoyant les lecteurs à la liste plus complète, annexée à la *Correspondance*. (Voir ci-dessus page XXVI et XXVII). *Les éditeurs.*

critique grossière de sa Mécanique qu'il n'entendait pas. M. Euler fit au Roi l'éloge de cet ouvrage, qu'il s'offrit de traduire, en y ajoutant les additions et les éclaircissements nécessaires. Ces additions ne renferment pas moins qu'une théorie complète du mouvement des projectiles; et il n'a rien paru dans l'espace de 38 ans, qui fut supérieur à ce que M. Euler a fait alors dans cette partie difficile des physico-mathématiques. Aussi le prix de cet excellent ouvrage a-t-il été généralement reconnu. Un ministre éclairé, feu M. Turgot, le fit traduire en français et introduire dans les écoles d'artillerie [1]; et presque en même-temps il en parut une traduction anglaise, faite avec tout le luxe dont la typographie est capable. En rendant, dans cet ouvrage, toute la justice possible au mérite de M. Robins, M. Euler relève modestement ses fautes contre la théorie, et se venge des anciens torts de son adversaire, en donnant à son ouvrage de la réputation. Je m'abstiens de toute réflexion sur la noblesse de ce procédé, si digne d'un grand homme. Qui pourrait lui refuser son admiration?

On sent bien qu'après avoir trouvé dans l'éther la cause de la flamme, de la pesanteur, de l'électricité et du magnétisme; après avoir même osé déterminer la petite résistance que ce fluide subtil oppose au mouvement des corps célestes, M. Euler ne pouvait guère être satisfait du système de l'émanation, établi par Newton pour expliquer les phénomènes de la lumière. L'examen de ce système précède la nouvelle théorie de la lumière et des couleurs que M. Euler publia en 1746.

Il y fait voir combien l'hypothèse du vide, adoptée par Newton, est en contradiction avec les émanations matérielles du soleil et des étoiles fixes, dont les rayons, en se croisant de toutes parts, rempliraient absolument tout l'espace, et opposeraient aux corps célestes une résistance bien plus grande que l'éther, dont ce grand homme niait par cette unique raison l'existence; il y montre, combien il est impossible que des particules matérielles puissent se mouvoir avec cette vitesse inconcevable, sans se troubler mutuellement dans leur cours; il calcule la perte de la matière solaire, et trouve que, dans peu de secondes, cette masse énorme serait dissipée en rayons; il tire enfin une autre objection, aussi forte que la précédente, de la structure des corps transparens qui, pour donner en tout sens un libre passage aux rayons matériels, devraient être destitués eux-mêmes de toute matière, c'est-à-dire, cesser d'être corps.

Descartes avait prétendu que la lumière nous parvient de la même manière que le son. Effectivement, on ne saurait méconnaître une analogie très marquée entre les sensations de l'ouie et de la vue, en réfléchissant qu'elles s'étendent toutes deux à des distances bien plus considérables que celles des autres sens; que le son et la lumière arrivent à nous par des lignes droites; et que l'un et l'autre peuvent être refléchis. M. Euler saisit cette ressemblance, et en poursuivant le parallèle, il fait voir, que la lumière naît d'un mouvement vibratoire dans l'éther, tout comme le son est produit par un pareil mouvement dans l'air; que la différence des couleurs, comme celle des sons, dépend de la fréquence des vibrations; et que le son, en passant par des corps propres à le transmettre, peut changer de direction et souffrir une espèce de réfraction, tout comme les rayons de lumière. Moyennant ce principe, étayé de tout ce qu'un raisonnement physique peut avoir de solide et de concluant, M. Euler est en état d'expliquer, de la manière la plus aisée et la plus conforme à la nature, tous les phénomènes de la lumière et de la vision; et même la différente réfrangibilité, que le système de Newton n'explique point, découle si naturellement de la théorie de M. Euler, qu'on pourrait en déduire ce phénomène *a priori*, s'il n'était pas connu par l'expérience.

Dans le même temps qu'il combattait le système de l'émanation, la philosophie Wolffienne était dans son plus grand éclat. On n'entendait parler que des monades et de la raison suffisante. L'étendue que Wolff et ses partisans donnèrent à ce dernier principe, ne fut pour Euler qu'un sujet de plaisanterie; mais le système des monades était une erreur ingénieuse, dont la destruction devait valoir une découverte aux yeux de l'ami de la vérité, accoutumé à n'admettre une opinion qu'après être remonté à ses premiers principes. Il fait voir, dans ses Pensées sur les élémens des corps, que les moindres particules n'en sauraient être plus petites que tout ce qu'on peut s'imaginer, sans être infi-

(1) Voyez la note suivante.

niment petites, ou rien; que les élémens de la matière, dont la force d'inertie est une propriété aussi générale que l'étendue et l'impénétrabilité, ne peuvent être doués de la force de changer continuellement d'état, aussi peu que les atomes d'Epicure; et qu'ainsi toutes les conclusions sur la diversité de ces forces, tirées du principe des Indiscernibles, tombent d'elles-mêmes. Après avoir détruit un système qui a eu, depuis, le sort de toutes les idées qui furent grandes sans être vraies, M. Euler substitua aux propriétés que Leibnitz et Wolff avaient attribuées aux monades, la force d'inertie, en faisant de cette essence de la matière, que Leibnitz avait déjà reconnue, le principe de tous les changemens qui arrivent dans le monde. Il se servit, dans la suite, du même principe, pour expliquer les effets du choc et de la pression, et il en fit usage pour démontrer qu'on ne saurait attribuer à la matière la faculté de penser.

La sortie contre les monades avait attiré à M. Euler plusieurs critiques, oubliées aujourd'hui, ainsi que le système dont elles s'efforçaient à prévenir la ruine. On n'en parle plus que lorsqu'on a besoin d'un exemple des égaremens auxquels l'esprit humain est exposé, quand il n'est guidé que par l'imagination.

Pour ce qui est du principe d'inertie dans lequel M. Euler fait consister toutes les forces, l'idée en est grande et conforme à la simplicité que la nature affecte dans toutes ses lois. Quoique la notion en soit purement métaphysique, ses effets sont du ressort de la géométrie: ils peuvent être calculés; et tout ce qu'on peut exiger d'une hypothèse, c'est qu'elle ne soit point contraire aux phénomènes qu'elle doit expliquer.

Ce serait ici le lieu de parler d'un grand nombre d'autres recherches philosophiques de M. Euler, où l'on verrait avec autant de plaisir que d'admiration la plus saine physique, unie à la géométrie la plus sublime. Mais les bornes de cet éloge nous obligent de passer sous silence les recherches sur la queue des comètes, sur l'aurore boréale et la lumière zodiacale, sur la propagation successive du son et de la lumière, sur l'espace et le temps, sur l'origine des forces, etc., tout comme nous avons omis le détail de tant de mémoires sur toutes les parties des mathématiques, pour ne nous occuper que des grands ouvrages de M. Euler qui n'est jamais descendu des hauteurs de l'analyse aux régions de la physique, sans y répandre du jour. Heureux et fécond dans la découverte de vérités importantes dans les sciences exactes, il ne le fut pas moins en expliquant des phénomènes dans la philosophie naturelle. Hardi dans les suppositions que le calcul pouvait justifier, il était circonspect dans les hypothèses qui n'en admettaient point. Cependant il en a fait de sublimes et de brillantes: le monde a prononcé sur le mérite des unes; la postérité prononcera sur le mérite des autres. L'historien a fait son devoir, quand il a indiqué ce qu'il y a de neuf dans les plus importantes de ces hypothèses.

Du philosophe nous retournons au géomètre. De toutes les connaissances utiles que les efforts combinés de l'analyse et de la géométrie peuvent élever à un certain degré de perfection, la navigation était la seule qui n'avait pas encore retiré du fruit de l'avancement universel des sciences physico-mathématiques. Il n'y avait guère que la partie hydrographique, et celle qui regarde la direction de la course des vaisseaux, qui eussent été traitées par les géomètres, conjointement avec l'astronomie nautique; à moins qu'on ne veuille compter les essais imparfaits de Huyghens et du chevalier de Renau, sur la manoeuvre des vaisseaux et sur leur vitesse. M. Euler fut le premier qui osa concevoir et exécuter le projet, de faire de la navigation une science complète. Un écrit sur le mouvement des corps flottans, imprimé dans les Mémoires des sciences et des beaux arts du mois d'avril 1735, et communiqué à l'Académie de St.-Pétersbourg par son auteur, M. de la Croix, lui en suggéra la première idée. Ses recherches sur l'équilibre des vaisseaux lui fournirent le moyen de ramener la stabilité à une mesure déterminée; le succès de ce premier essai l'encouragea à traiter à fond toute la science navale, et il composa le grand ouvrage que notre Académie a fait publier en 1749. On y trouve, dans un ordre systématique, tout ce que la théorie de l'équilibre et du mouvement des corps flottans et celle de la résistance des fluides ont de plus difficile et de plus sublime.

Mais ces principes généraux ne suffisent pas. Il s'agit, dans la navigation, de corps flottans d'une figure déterminée. Il faut non seulement calculer la résistance et les forces, il faut savoir diminuer l'une et augmenter les autres,

autant qu'il est possible; et en garantissant le vaisseau des efforts de l'eau pour l'arquer et pour le balancer, lui donner la figure qui réunit tous les avantages possibles, et qui le met en état de remplir en tous points sa destination.

Ainsi, indépendamment de ce que la théorie peut nous enseigner sur la construction des vaisseaux et leur manoeuvre en général, il faut qu'elle nous instruise aussi des moyens de concilier entre elles les différentes propriétés que le navire bien construit doit avoir. Il y en a qu'on n'obtient que par des sacrifices: la plus grande stabilité, par exemple, et la course la plus rapide ne sauraient se trouver ensemble. Il est donc de la dernière importance de savoir, combien il faut sacrifier d'un avantage, pour obtenir tous les autres, autant que la destination différente des vaisseaux l'exige. C'est ce qu'enseigne la seconde partie de l'ouvrage de M. Euler, où il a rassemblé tout ce que l'art du pilote et du constructeur pouvait espérer du perfectionnement de la théorie. Il a enrichi, dans la suite, cette partie intéressante des mathématiques de plusieurs vues ingénieuses et utiles, dans beaucoup de mémoires, insérés dans les collections des Académies de St.-Pétersbourg, de Paris et de Berlin, et principalement dans les deux mémoires sur la manière de suppléer à l'action du vent et sur les effets du roulis et du tangage, dont le dernier a remporté, en 1759, le prix de l'Académie de Paris.

L'architecture navale qui, par le défaut de principes sûrs, avait été obligée de s'en tenir si longtemps aux lois de la routine, et qu'une longue expérience n'avait pu garantir de bien des fautes dans la construction des vaisseaux et dans leur mâture, se vit donc tout-d'un-coup enrichie d'une théorie complète, que d'autres arts n'ont eu l'avantage de recevoir qu'après bien des tentatives et par des gradations presque insensibles.

Mais cette théorie est écrite dans une langue qui n'est pas familière aux gens du métier; elle suppose des connaissances mathématiques qu'on ne saurait guère attendre du constructeur ni du pilote. La pratique ne pouvait donc retirer aucun fruit des importantes découvertes de M. Euler, à moins qu'on ne trouvât moyen de les dégager des calculs trop profonds, des recherches trop difficiles et trop compliquées. Il sentit cet inconvénient dans la suite; et de fréquens entretiens qu'il eut, après son retour à St.-Pétersbourg, avec feu l'amiral Knowles, le déterminèrent à écarter de cette théorie tout ce qui n'est pas intimement lié avec la science des marins, et tout ce qui n'est pas à leur portée, et il publia, en 1773, sa Théorie complète de la construction et de la manoeuvre des vaisseaux, mise à la portée de tous ceux qui s'appliquent à la navigation.

Jamais ouvrage de géomètre n'eut un succès plus brillant: on en fit d'abord une nouvelle édition à Paris, on l'introduisit dans les écoles de marine(1); et le Roi récompensa M. Euler, par une gratification de 6000 livres, du bien que ses nombreuses découvertes ont fait à la nation française comme à toutes les nations éclairées: ce sont les expressions des éditeurs de Paris. Il parut aussi, presque en même temps, une traduction italienne, anglaise et russe

(1) Les marques d'estime qu'un homme vertueux et éclairé témoigne au vrai mérite, honorent trop celui qui les donne et celui qui les reçoit, pour que je ne me fasse un devoir de publier, à cette occasion, ce que feu M. Turgot a écrit à M. Euler, en lui notifiant les ordres de son Roi; le voici:

à Fontainebleau le 15 Oct. 1775.

«Pendant le temps, Monsieur, que j'ai été chargé du département de la marine, j'ai pensé que je ne pouvais rien faire de mieux pour l'instruction des jeunes gens élevés dans les écoles de la marine et de l'artillerie, que de les mettre à portée d'étudier les ouvrages que Vous avez donnés sur ces deux parties des mathématiques: j'ai en conséquence proposé au Roi, de faire imprimer, par ses ordres, Votre traité de la construction et de la manoeuvre des vaisseaux, et une traduction française de Votre commentaire sur les principes d'artillerie de Robins.»

«Si j'avais été à portée de Vous, j'aurais demandé Votre consentement, avant de disposer d'ouvrages qui Vous appartiennent; mais j'ai cru que Vous seriez bien dédommagé de cette espèce de propriété par une marque de la bienveillance du Roi. Sa Majesté m'a autorisé à Vous faire toucher une gratification de mille roubles, qu'elle Vous prie de recevoir comme un témoignage de l'estime qu'elle fait de Vos travaux et que Vous méritez à tant de titres.»

«Je m'applaudis, Monsieur, d'en être dans ce moment l'interprète, et je saisis avec un véritable plaisir cette occasion de Vous exprimer ce que je pense, depuis longtemps, pour un grand homme qui honore l'humanité par son génie et les sciences par ses moeurs. Je suis etc.»

Turgot.

de cet excellent ouvrage, et M. Euler reçut, à l'occasion de la dernirée, un présent de 2000 roubles de la part de notre grande Souveraine.

Nous avons rassemblé ici les principaux travaux de notre géomètre, qui roulent sur un même objet, quoique le dernier n'ait été fait que longtemps après son retour à St.-Pétersbourg; parce qu'il est intéressant de voir, d'un seul coup-d'oeil, combien de services il a rendus à la navigation, c'est-à-dire, à l'une des plus sublimes et des plus utiles connaissances de l'esprit humain.

En 1749, le Roi chargea M. Euler de visiter le canal de Funo, entre l'Havel et l'Oder, pour remédier à certains inconvéniens qu'il y avait remarqués. En parcourant un recueil de cinquante-quatre lettres que le Roi lui a écrites, depuis 1741 jusqu'en 1777, parmi lesquelles il y en a plusieurs de la propre main de Sa Majesté, j'ai vu qu'on s'est servi bien des fois plus particulièrement de ses lumières. En examinant les calculs des salines de Schönebek, des machines d'eau de Sans-Souci et de plusieurs projets de finances, il eut l'occasion de rendre à l'état des services réels et immédiats, en lui épargnant des dépenses aussi onéreuses qu'inutiles. Aussi le Roi s'est-il souvent adressé à lui, avec la confiance la plus entière, pour ce qui concernait les affaires de l'Académie de Berlin et de l'Université de Halle. (1).

Il était temps de rassembler, dans un ouvrage systématique et suivi, le grand nombre de découvertes importantes que M. Euler avait faites sur l'analyse infinitésimale, dans le cours de trente ans, et qui se trouvent éparses dans les collections académiques. Il en avait conçu le projet; mais avant que de l'exécuter, il fallait préparer le monde, capable de saisir ces sublimes leçons, par un ouvrage préliminaire, où l'on pût puiser toutes les notions que cette étude exige. Il composa, pour cet effet, son Introduction à l'analyse des infiniment-petits, où il a épuisé toute la doctrine des fonctions, soit algébriques, soit transcendentes, en montrant leur transformation, leur résolution et leur développement. Il y recueillit tout ce qu'il avait trouvé d'utile et d'intéressant sur les propriétés des séries infinies et leur sommation; il y ouvrit une nouvelle route pour traiter les quantités exponentielles, et en déduisit le moyen de fournir une idée plus nette et plus féconde des logarithmes et de leur usage; il y exposa le nouvel algorithme qu'il avait trouvé pour les quantités circulaires, et dont l'introduction a fait une nouvelle révolution dans toute la science du calcul; et après avoir montré l'utilité du calcul des sinus, dont il est le véritable auteur, et l'usage des séries recurrentes, il donne, dans la seconde partie, la théorie générale des lignes courbes, avec leurs divisions et subdivisions, et dans un supplément, la théorie des solides et de leurs surfaces, en montrant comment leur mesure conduit aux équations à trois variables; et il termine enfin cet important ouvrage en développant l'idée des courbes à double courbure, que lui fournit la considération de l'intersection des surfaces curvilignes.

A cette introduction succédèrent, dans la suite, ses Leçons de calcul différentiel et celles de calcul intégral, publiées par notre Académie que M. Euler ne cessait de regarder comme propriétaire légitime de ses grands ouvrages. Le principal mérite du premier de ces ouvrages, qui roule sur la partie du calcul infinitésimal, déjà perfectionnée par ses inventeurs, Newton et Leibnitz, et par les Bernoulli, consiste dans le point de vue d'où M. Euler en a envisagé les véritables principes, dans l'ordre systématique avec lequel il les a exposées, dans l'esprit de méthode qui y règne, dans la clarté avec laquelle il y a montré l'utilité de ce calcul, par rapport à la doctrine des séries et à la théorie des plus-grands et des plus-petits. Ses découvertes sont entremêlées avec celles des premiers inventeurs; mais les traces du génie, dont l'essence est de découvrir, sont indélébiles; même dans les objets où il ne saurait

(1) Après la mort du baron de Wolff, il s'agissait de le remplacer dans l'Université de Halle; le Roi écrivit à M. Euler à ce sujet: celui-ci lui proposa d'abord M. Daniel Bernoulli, et après le refus de cet illustre savant, M. de Segner, qui eut cette place à des conditions très avantageuses que lui procura M. Euler, en déterminant le Roi, en même-temps, d'acheter pour l'Université l'appareil physique de feu M. de Wolff. C'est aussi à M. Euler que le Roi s'adressa pour engager feu M. de Haller à entrer dans son service, en lui offrant une place dans la même Université. Les conditions déplurent au Roi, et le projet échoua.

exercer cette faculté, il tâche de perfectionner au moins les inventions d'autrui, de ramener les principes connus à un plus haut degré d'évidence et de simplicité, ou d'en tirer de nouvelles conséquences. Qui pourrait méconnaître ce caractère dans les ouvrages de M. Euler? Il y a partout du sien; mais le détail en serait trop long pour les bornes de cet éloge.

Le calcul intégral, dont les premiers pas se perdent dans l'origine du calcul des différences, est loin du degré de perfection que ce dernier a atteint. Il n'y a point, comme dans la décomposition des grandeurs, des règles générales, pour remonter des élémens aux grandeurs mêmes. Si jamais ces règles se trouvent, la postérité rendra à M. Euler la justice d'en avoir préparé la découverte, par le grand nombre d'intégrations difficiles dont lui seul est venu à bout. Sa gloire est d'avoir reculé les bornes de ce calcul sublime loin au-delà de l'attente des premiers inventeurs; et Newton, s'il pouvait revenir, serait surpris des difficultés extrêmes que cet homme étonnant a su vaincre.

Le troisième volume de son Calcul intégral contient le nouveau genre de calcul dont il a enrichi l'analyse infinitésimale: celui des variations. J'ai déjà remarqué que le problème des isopérimètres lui en avait fourni la première idée. Elle fut saisie par M. de la Grange, digne successeur de M. Euler dans l'Académie de Berlin: il la dégagea de toutes les considérations géométriques; il en fit un problème d'analyse, et parvint à le résoudre par le nouveau genre de calcul que M. Euler a tant perfectionné depuis, et qu'il a nommé calcul des variations, parce que le rapport entre les quantités variables y est regardé lui-même comme variable.

Nous avons déjà vu, que le génie de M. Euler était trop vaste pour se contenir toujours dans les bornes des mathématiques, quelque étendues qu'elles soient. Tout ce qui y avait le moindre rapport, il le crut de son ressort; tout ce qui était mesurable, il le soumit à ses calculs. Nous allons voir, combien la physique, l'optique et l'astronomie doivent à la fois à sa théorie de la lumière et des couleurs.

L'examen de la théorie Newtonienne lui avait fourni l'occasion de faire des recherches sur la différente réfrangibilité des rayons de lumière, et sur le mauvais effet que la dispersion des couleurs produisait dans les télescopes à réfraction, qu'on avait été obligé d'abandonner presque entièrement à cause de ce défaut. La considération de la structure merveilleuse de l'oeil lui fit imaginer qu'une certaine combinaison de divers corps transparens pourrait remédier à cet inconvénient. Il proposa, pour cet effet, en 1747, des objectifs composés de deux verres dont la cavité pût être remplie d'eau.

Son sentiment fut attaqué par le fameux artiste anglais, Dollond, qui lui opposa l'autorité de Newton; M. Euler ne tarda pas à lui montrer la fausseté de ses principes. Quelques expériences, faites sur des ménisques dont la cavité pouvait être remplie de différentes liqueurs, le confirmèrent dans son opinion, et M. Dollond, qui avait trouvé, en attendant, deux sortes de verres, propres à l'examiner de plus près, couronna enfin, en 1757, la conjecture heureuse de M. Euler par l'invention des lunettes achromatiques, qui ont fait époque dans l'astronomie et dans la dioptrique.

Les succès de M. Dollond qui se servit, avec tant d'avantage, d'une découverte qu'il avait d'abord attaquée comme contraire à l'expérience, engagèrent M. Euler à pousser plus loin ses recherches sur les instrumens dioptriques, à remédier aux défauts qui leur viennent de l'aberration des rayons, engendrée par la figure sphérique des verres, et à donner enfin des règles générales pour la construction des télescopes et des microscopes, de la solidité desquelles il s'était convaincu par l'expérience, en faisant construire des lunettes d'après sa nouvelle théorie. ([1]).

(1) Le Roi, à qui il en avait envoyé quelques-unes, construites d'après ses principes, applaudit à ce travail utile et lui adressa de Waldau la lettre suivante, d'autant plus remarquable, qu'elle est écrite en entier de la main de Sa Majesté:

«Je vous remercie des petites lunettes d'approche qui me sont arrivées à la suite de votre lettre du 14 de ce mois; et je loue le soin que vous prenez de rendre utile aux hommes la théorie que vous fournit votre étude et votre application aux sciences. Comme mes occupations présentes ne me permettent pas de les examiner avec l'attention que mérite tout ce qui me vient de votre part, je me réserve à le faire quand j'en aurai plus de loisir. Sur ce je prie Dieu qu'il vous ait en Sa sainte et digne garde. Waldau ce 15 Septembre 1759.

Féderic.

C'est donc à cette controverse avec Dollond, qu'on est redevable d'une des plus importantes découvertes qui aient été faites dans ce siècle. Elle a rendu aux astronomes de très grands services, en leur montrant au ciel de nouveaux phénomènes, et en facilitant le travail des observations.

La controverse entre MM. Euler, d'Alembert et Bernoulli au sujet du mouvement des cordes vibrantes, ne peut intéresser proprement que les géomètres de profession. M. D. Bernoulli, qui fut le premier à en développer la partie physique qui regarde la formation du son engendré par ce mouvement, crut la solution de Taylor suffisante pour l'expliquer. MM. Euler et d'Alembert, qui avaient épuisé, dans cette matière difficile, tout ce que l'esprit analytique a de sublime et de profond, firent voir que la solution de M. Bernoulli, tirée des Trochoïdes Taylorien-nes, n'est pas générale, qu'elle est même insuffisante. Cette controverse qui a été continuée longtemps, avec tous les égards que des hommes aussi illustres se doivent mutuellement, a donné naissance à quantité d'excellens mémoires; elle n'a fini proprement qu'à la mort de M. Bernoulli (1).

Une autre controverse qui ne dura pas tant, mais qui se fit avec plus d'aigreur de part et d'autre, ce fut celle avec M. Koenig, qui avait attaqué, en 1751, le principe de la moindre action de M. de Maupertuis, à qui il contestait l'honneur d'en être le premier inventeur. Mais comme elle ne roulait pas sur une découverte faite par M. Euler lui-même, il suffit de remarquer à son honneur, qu'il y a pris, avec la chaleur d'un véritable ami, le parti de M. de Maupertuis, et que quelques excellens mémoires, sortis de la main de celui qui n'en a jamais fait d'autres, ont dû leur origine à cette dispute.

La solution du problème important de la précession des équinoxes et de la nutation de l'axe de la terre, que M. d'Alembert a été le premier à résoudre, engagea M. Euler à publier ses recherches sur cette matière dans le cinquième volume des mémoires de Berlin, le même ou se trouve l'heureux dénouement de la controverse entre Leibnitz et Bernoulli sur les logarithmes des nombres négatifs et imaginaires. Ce problème de la précession des équinoxes engagea M. Euler à faire des recherches sur le mouvement de rotation des corps solides, en tant que l'axe de rotation est variable; mouvement pour lequel les principes de mécanique, connus jusqu'alors, n'étaient pas suffisans. Il fallait donc remonter aux premiers principes de la doctrine du mouvement, et voir si l'on ne pourrait pas en déduire les règles générales pour la détermination du mouvement d'un corps solide dont l'axe de rotation est mobile. Il le fit, et découvrit un nouveau principe de mécanique, moyennant lequel il fut en état de traiter, dans toute sa généralité, le problème du mouvement des corps solides.

Ces recherches, propres à répandre un nouveau jour sur toute la science du mouvement, méritaient d'être exposées dans toute leur étendue. Dans son grand ouvrage sur la mécanique, M. Euler n'avait traité que le mouvement des corps infiniment petits; il réservait la partie la plus difficile et la plus essentielle, celle du mouvement des corps solides, pour un ouvrage séparé, qui parut enfin en 1765, et qui peut être regardé comme un traité complet de mécanique, puisqu'il renferme, en forme d'introduction, tous les principes du mouvement des points, traités d'une manière nouvelle et préférable à celle que l'auteur avait suivie autrefois. A la suite de ces principes on trouve rassemblées toutes les découvertes importantes qu'il avait faites sur les mouvemens des corps solides. Ce sont ces

(1) J'avais communiqué à M. Bernoulli, en 1776, une nouvelle méthode de M. Euler, encore plus générale que toutes les précédentes, parce qu'elle s'étendait à des figures initiales quelconques, dont la nature ne peut pas même être représentée par aucune équation. L'extrait suivant de sa réponse fera voir le point où la controverse était alors, et la noblesse des procédés de deux grands hommes qui sont d'opinion différente:

«L'esquisse que Vous me faites de la méthode de M. Euler m'a fait plaisir; mais elle n'a change en rien mes idées sur cette matière; je suis toujours persuadé que ma méthode donne *in abstracto* tous les cas possibles; j'avoue cependant que, dans certains points de vue, celle de M. Euler est fort préférable à la mienne; mais il y a aussi d'autres points de vue pour le contraire, puisque ma méthode peut être appliquée à tel nombre de corps fini qu'on propose, lors même que, dans le système, il n'y a aucun retour parfait ou période à attendre. Quoi qu'il en soit de mes pretentions, je suis toujours prêt de baisser pavillon devant mon amiral»

découvertes qui l'ont mis en état d'apporter tant de perfection à la théorie du mouvement des corps célestes, et à rendre par là de si grands services à l'astronomie et à la navigation.

M. Euler n'avait cessé, pendant tout son séjour à Berlin, de rendre des services très signalés à l'Académie impériale, soit en lui vouant la plus grande et la plus importante partie de ses travaux littéraires, soit en veillant à ses intérêts économiques, ou en se chargeant de l'instruction de ses élèves[1]. Il n'a donc point cessé le lui appartenir à tous les titres; et il faut croire qu'on a pensé de même à la cour et à l'armée de Russie, en lui accordant des sauvegardes, et en le dédommageant de toutes les pertes qu'il avait souffertes dans la dernière guerre à sa campagne, pendant le séjour des troupes russes à Berlin.

Avec cette prédilection marquée pour le pays où il avait passé les premières années de son adolescence, et pour le corps où il avait vu naître sa célébrité, M. Euler devait naturellement nourrir le désir d'y retourner. L'avènement de Catherine-la-Grande au trône de Russie, l'éclat de son règne aussi sage que doux, aussi juste que bienfaisant, avaient rempli le monde d'une admiration universelle; et la protection qu'elle accordait aux sciences et à ceux qui les cultivent, avaient donné de nouvelles forces à l'Académie, et contribué à raffermir M. Euler dans la résolution de finir ses jours au service de cette incomparable princesse, née pour faire le bonheur de ses sujets et l'admiration de l'univers.

Le mois de mai 1766 fut l'époque où il se vit près de l'accomplissement de ses voeux. Le ministre de Russie à Berlin, prince Dolgorouky, lui accorda, au nom de l'Impératrice, toutes les conditions qu'il avait faites, soit pour lui soit pour sa famille, à laquelle il assura par là un état avantageux. Ce ne fut qu'avec une peine extrême qu'il obtint son congé pour lui et pour ses deux fils aînés. Le Roi refusa absolument au cadet la permission d'accompagner son père.

Au mois de juin suivant, M. Euler quitta donc Berlin, où il avait joui pendant 25 ans d'une considération proportionnée à son mérite éminent. Les princes de la maison royale, et particulièrement le margrave régnant de Brandenbourg-Schwedt[2], le virent partir à regret, et ils le lui témoignèrent d'une manière flatteuse.

Il était à la veille de partir, quand le prince Adam Czartorisky l'invita au nom du Roi de Pologne à prendre la route de Varsovie, où il passa dix jours avec tous les agrémens que les attentions d'un prince gracieux peuvent répandre sur la vie d'un philosophe, qui sait en jouir sans les rechercher[3]. Il revit donc St.-Petersbourg, après une longue absence, le 17 juillet 1766. Il fut d'abord présenté, avec ses deux fils aînés, à Sa Majesté impériale, et la première grâce qu'il obtint de sa souveraine, ce fut le congé de son cadet, qu'il lui fut facile d'obtenir moyennant une aussi puissante intercession.

(1) Il recevait dans sa maison les élèves que l'Académie envoyait à Berlin pour étudier les mathématiques. MM. Kotelnikov et Roumovsky y ont passé plusieurs années sur ce pied, et ont joui des instructions de ce maître incomparable.

(2) A l'habitude d'un commerce fréquent et familier, que ce prince eut avec lui, et à l'amitié intime qui en était l'effet, se joignirent, pour le lui faire sincèrement regretter, les sentimens d'une reconnaissance particulière pour tout ce que M. Euler avait contribué à la culture de l'esprit des princesses, filles du margrave. Il leur avait donné des leçons; et c'est à elles qu'il a écrit, pendant le séjour de la cour à Magdebourg, les lettres sur différens sujets de physique et de philosophie, qu'il a fait publier après son retour à St.-Pétersbourg.

(3) Il a conservé, pendant toute sa vie, le tendre souvenir des bontés que le Roi lui a témoignées; et l'attachement respectueux que lui avaient inspiré les qualités du coeur et de l'esprit de ce prince gracieux, s'est perpétué par le commerce de lettres qu'il a eu l'honneur d'entretenir avec lui. Je ne puis résister à l'envie d'orner cet éloge d'une de celles que le Roi lui écrivit, en 1772:

«Monsieur le professeur Euler, En répondant à votre lettre du 4 août dernier, j'aurais bien souhaité de pouvoir confirmer l'opinion que vous avez des circonstances plus heureuses, sur lesquelles votre amitié pour moi vous a dicté l'expression d'un coeur vertueux et sensible. Mais . . . .
. . . . Je vous remercie cependant de votre bonne volonté à cet égard, et je passe à la reconnaissance que je dois à vos soins, pour me communiquer les observations que les habiles astronomes de votre Académie ont faites à Bender et vers les embouchures du Dniestr et du Danube,

A peine installé dans sa maison, pour l'achat de laquelle Sa Majesté impériale lui avait fait présent de 8000 roubles, il fut attaqué d'une maladie violente, dont il ne revint qu'avec la perte totale de la vue. Une cataracte qui s'était formée dans l'oeil gauche, le priva entièrement de l'usage d'un organe que trop d'application avait gâté.

Quel accident pour un homme à qui l'habitude avait fait du travail une espèce de besoin, et dont l'esprit, sans cesse agité de quelque nouvelle découverte, se voit tout d'un coup hors d'état de poursuivre ses travaux! C'eût été le sort de tout autre que M. Euler: sa prodigieuse mémoire et son imagination étonnante, augmentées par la concentration de toutes les forces d'un esprit dégagé de la sensation distrayante des objets extérieurs, suppléèrent bientôt à une perte qui paraissait devoir finir la carrière littéraire de cet homme illustre.

Un garçon tailleur qu'il avait amené avec lui de Berlin en qualité de domestique, et qui n'avait aucune teinture des mathématiques, fut l'écrivain auquel il dicta ses Elémens d'algèbre, si généralement admirés tant pour les circonstances dans lesquelles ils furent composés, que pour le degré suprême de clarté et de méthode qui y règne. L'esprit inventeur se décèle encore dans cet ouvrage purement élémentaire. C'est le seul où l'on trouve une théorie suivie de l'analyse de Diophante; on en a vu paraître, peu de temps après, une traduction russe et française.

L'arrivée de M. Krafft le mit en état d'exécuter un projet qu'il avait roulé longtemps dans la tête: celui de réunir, en un seul corps d'ouvrage, tout ce qu'il avait fait, dans l'espace de trente ans, pour le perfectionnement des instrumens d'optique et de leur théorie. Il mit la main à l'exécution de ce travail avec sa vivacité ordinaire et fit publier en 1769, 1770 et 1771 trois gros volumes sur la Dioptrique.

Le premier volume contient la théorie générale de cette nouvelle science: car on ne peut pas dire qu'elle ait existé avant l'époque préparée par M. Euler. La longueur excessive qu'on avait été obligé de donner aux lunettes, avant la découverte des objectifs composés, et la confusion des images avaient obligé les astronomes de les abandonner presqu'entièrement et de se borner à l'usage des télescopes à réflexion. Le calcul de la construction la plus avantageuse de l'une et de l'autre espèce de ces instrumens était un cahos; et quoique ce problème n'appartienne proprement qu'à la géométrie élémentaire, et qu'il n'exige que fort peu de connaissances de l'analyse infinitésimale, on était resté extrêmement en arrière: et ce n'est que depuis que M. Euler a commencé à s'en occuper, qu'on peut dater les progrès de cette science.

Le second et le troisième volume de son ouvrage renferment les règles pour la meilleure construction des lunettes, des télescopes catopriques et des microscopes. Le calcul de l'aberration des rayons, engendrée par la sphéricité des verres, est un chef-d'oeuvre de l'analyse la plus raffinée. On est forcé d'admirer le grand art, avec lequel M. Euler a su employer cette analyse pour concilier à toutes les espèces d'instrumens tous les avantages possibles: la plus grande clarté de l'image, le plus grand champ apparent, la plus grande diminution de longueur, pour tous les grossissemens possibles et pour tel nombre d'oculaires qu'on veut employer. Toutes les espèces d'instrumens optiques se trouvent examinées et calculées dans cet ouvrage, avec une simplicité sans exemple dans des recherches rebutantes jusqu'alors, par la longueur des calculs et par la quantité d'élémens qui y entrent.

Dans le même temps que l'Académie fit publier cet ouvrage important, ses presses étaient occupées à imprimer les lettres à une princesse d'Allemagne, le calcul intégral, les élémens d'algèbre, les calculs de la comète de 1769, celui de l'éclipse du soleil et du passage de Vénus de la même année, la théorie nouvelle de la lune et celle de la navigation, sans compter le grand nombre de mémoires qui se trouvent dans les volumes des Commentaires de ce temps-là.

avec les positions de quelques endroits également importans pour la géographie. Je tâche de les mettre à profit pour perfectionner celles qui se font dans ce pays-ci avec assez d'application et de succès, malgré les troubles qui mettent un grand obstacle au progrès des sciences. Je vous en demande la continuation, autant pour l'utilité publique que pour ma satisfaction particulière, et désirant des occasions pour vous en donner des marques effectives, je prie Dieu, qu'il vous ait, monsieur le professeur Euler, en sa sainte et digne garde.»

Fait à Varsovie, le 7 juin 1772.

Stanislas Auguste Roi.

A peine le premier de ces ouvrages eut-il paru, que M. Roumovsky le traduisit en Russe. On en fit aussi une nouvelle édition à Paris, et une traduction allemande à Leipzig. Pour ce qui regarde son contenu, il suffit de remarquer que, comme il est à la portée d'un plus grand nombre de lecteurs, et même à la portée du beau sexe, il n'a pas peu contribué à répandre le nom illustre de son auteur, et à le rendre cher à ceux qui ne peuvent le juger que d'après ses lettres à une princesse d'Allemagne.

L'année 1769 sera à jamais mémorable dans l'histoire du progrès des sciences, par le concours heureux des grands de la terre, à mettre les astronomes en état de profiter du passage de Vénus sur le disque du soleil. L'Impératrice de Russie, les Rois de France, d'Angleterre et d'Espagne envoyèrent des astronomes dans toutes les parties du monde, pour observer ce phénomène, si rare et si important pour fixer les dimensions du système solaire. Dix astronomes, animés par la gloire de prendre part à cet événement, et encouragés par la protection de notre auguste Souveraine, se dispersèrent dans le vaste empire de Russie, pendant que M. Euler méditait une nouvelle méthode de tirer parti de leurs observations pour déterminer la véritable parallaxe du soleil, et par conséquent les distances de toutes les planètes. Il en trouva une très élégante pour calculer non seulement les observations du passage, mais encore celles de l'éclipse du soleil qui suivit de près le premier phénomène, et dont heureusement on pouvait se servir pour déterminer la position géographique des lieux des observations. Le calcul de toutes ces observations a été fait par M. Lexell, d'après cette méthode; on peut donc dire que c'est encore à M. Euler que l'astronomie est redevable du degré de perfection qu'elle a tiré de la détermination exacte de la parallaxe du soleil.

Les recherches sur la lune ont occupé une partie considérable de son temps. Il avait déjà publié, en 1746, des tables de la lune et, en 1753, une théorie de ses mouvemens, de laquelle feu M. Mayer a fait usage, dans la suite, pour calculer les tables dont les astronomes se servent aujourd'hui, et qui lui ont valu le prix pour la longitude. Le parlement anglais fit payer, en même temps, à M. Euler une gratification de 300 livres sterl. pour le récompenser d'avoir fourni à M. Mayer les théorèmes, moyennant lesquels il a été en état de contribuer au problème important des longitudes. (1)

Cependant l'Académie de Paris qui, depuis qu'elle s'était associé M. Euler(2), avait couronné trois de ses mémoires sur les inégalités dans les mouvemens des planètes, choisit, pour sujet des prix de 1770 et 1772, la perfection de la théorie de la lune, et M. Euler, aidé par son fils ainé qui avait déjà partagé le prix de 1761 sur l'arrimage des vaisseaux, remporta l'un et l'autre.

(1) La reconnaissance qu'une nation éclairée témoigne au vrai mérite, est à la fois et trop flatteuse pour le grand homme qui en est l'objet, et trop encourageante pour ceux qui marchent sur ses traces, pour ne pas la consigner dans ce discours, en y insérant un extrait de la lettre que M. Euler reçut à cette occasion du secrétaire du bureau des longitudes:

Admiralty Office. London, 13 June 1765.

«Sir, the Parliament of Great-Britain having, by an act passed in their late sessions (a printed copy of which I herewith transmit to you) been pleased to direct, that a sum of money, not exceeding three hundred pounds in the whole, shall be paid to you, as a reward for having furnished theorems, by the help of which the late Mr. Professor Mayer of Goettingen constructed his lunar tables, by which tables great progress has been made towards discovering the longitude at Sea. I am directed by the Commissioners of the longitude to acquaint you therewith and to congratulate you upon this honorary and pecuniary acknowledgement, directed to be made you by the highest Assembly of this nation, for your useful and ingenious labours towards the said discovery etc.»

(2) On sait que le nombre des associés externes de l'Académie de Paris est fixé à huit; M. Euler en fut nommé le neuvième, sans qu'il y eût, par conséquent, de place vacante. Les circonstances qui ont accompagné cette réception, méritent d'être consignées dans cet éloge; elles se trouvent rapportées dans la lettre suivante du marquis d'Argenson:

à Versailles, le 15 juin 1755.

«Le Roi vient de Vous choisir, Monsieur, d'après les voeux de son Académie royale des sciences, pour remplir une place d'associé externe dans cette Académie; et comme elle a nommé en même temps Mylord Maclesfield, président de la société royale de Londres, pour remplir une pareille place, qui vaque par la mort de M. Moivre, Sa Majeste a décidé que la première place de cette espece qui vaquera, ne sera pas remplie. L'extrême rareté de

Il avait trouvé moyen, dans son dernier mémoire, de tenir compte de plusieurs inégalités du mouvement de la lune, qu'il n'avait pas été en état de déterminer dans sa première théorie, à cause de la complication des calculs, qu'entrainait la méthode dont il s'était servi alors. Il eut le courage de refondre toute la théorie avec MM. J. A. Euler, Krafft et Lexell, et de poursuivre ses recherches jusqu'à la construction de nouvelles tables, qui ont paru conjointement avec le grand ouvrage publié en 1772. Au lieu de s'arrêter, comme autrefois, à l'intégration infructueuse des trois équations différentielles du second degré que les principes mécaniques fournissent, il les rapporta d'abord aux trois coordonnées qui déterminent le lieu de la lune; il distribua toutes les inégalités de la lune en classes, en tant qu'elles dépendent ou de l'élongation moyenne du soleil et de la lune, ou de l'excentricité, ou de la parallaxe, ou de l'inclinaison de l'orbite lunaire. Tous ces moyens, employés avec art, et accompagnés de tous les artifices de calcul que le premier analyste du monde était seul capable d'imaginer, réussirent au-delà de toute attente. On est saisi d'étonnement à la vue de ces calculs immenses, et de la richesse des ressources employées pour les abréger et pour faciliter l'application au vrai mouvement de la lune.

La patience et la tranquillité d'esprit que ce travail énorme exigeait, nous surprendra d'avantage, si nous nous rappelons dans quelles circonstances et en quel temps il a été fait. Privé de la vue, obligé de faire la disposition de tous ces calculs immenses par la seule force de sa mémoire et de son imagination, arriéré dans ses affaires domestiques par un incendie qui venait de ravir à lui et à sa famille une grande partie de leurs biens, réduit à la nécessité de quitter une maison ruinée, où tous les coins lui étaient connus, où l'habitude avait suppléé, par conséquent, à la vue, excédé des troubles que des changemens si tristes et si soudains et le rétablissement de sa maison (1) durent lui causer: M. Euler fut en état de composer un ouvrage qui tout seul suffirait pour l'immortaliser, l'eût-il fait dans la situation la plus riante et la plus tranquille. Je ne connais rien de plus fort, rien qui tienne plus de l'héroisme, que cette égalité d'ame, ce courage inébranlable au milieu des revers de la fortune.

Peu de mois après ce malheureux accident, dont la générosité de Sa Majesté impériale allégea le poids par un présent de 6000 roubles, M. Euler se fit opérer la cataracte par le célèbre oculiste, baron de Wentzel, et cette opération lui rendit la vue, à sa grande satisfaction et à celle de toute sa famille. Mais cette joie fut peu durable: négligeant les précautions nécessaires, et trop pressé, peut-être, à faire usage d'un organe qu'il aurait dû avoir appris à ménager, il le perdit pour la seconde fois au milieu des souffrances les plus affreuses.

Il fut donc réduit de nouveau à la nécessité de se servir des yeux d'autrui, avant que d'avoir pu faire usage de l'oeil que l'opération lui avait rendu pour quelque temps. Ses fils, le professeur et le lieutenant-colonel, et MM. Krafft et Lexell continuèrent de lui prêter alternativement les leurs, soit pour l'exécution de ses grands ouvrages, soit pour ce grand nombre de mémoires qu'on trouve dans les derniers volumes des Nouveaux Commentaires, et dont je m'abstiens de parler, de crainte d'abuser de la patience de cette assemblée.

Je m'arrêterai pourtant un instant à ceux qui roulent sur l'équilibre et le mouvement des fluides et sur la perfection ultérieure des lunettes achromatiques.

ces sortes d'arrangemens est une distinction trop marquée pour ne pas Vous en faire l'observation, et Vous assurer de toute la part que j'y prends. L'Académie désirait vivement de Vous voir associé à ses travaux, et Sa Majesté n'a pu qu'adopter un témoignage d'estime que Vous méritez à si juste titre. Soyez persuadé, Monsieur, qu'on ne peut pas Vous être plus parfaitement dévoué que je le suis»

M. d'Argenson.

Si j'ai inséré cette lettre et quelques autres, prises d'un grand nombre de lettres que M. Euler a reçues de personnes illustres, soit par leur rang, soit par leurs talens, ce n'est pas certainement dans l'intention de grossir cet éloge, ni de lui prêter par là un mérite que je n'ai pu lui donner moi-même: c'est que j'ai cru ces pièces dignes d'y entrer, et je pense qu'on les y verra avec plaisir. Si elles n'ajoutent rien au mérite d'un grand homme, on les estimera comme des marques de la justice qui lui fut rendue comme tel.

(1) Le brouillon de la pièce de concours se perdit à cette occasion, et M. Euler le fils se vit obligé de repasser toute la théorie de la lune et d'en faire tous les calculs pour la seconde fois.

Depuis l'Hydrodynamique de M. Daniel Bernoulli, la perfection du calcul qui, entre les mains de M. Euler, devenait de jour en jour plus riche et plus applicable aux questions les plus difficiles des sciences physico-mathématiques, avait été tellement augmentée, qu'on était en droit de s'attendre à le voir appliqué aussi à cette partie essentielle de la science du mouvement. M. Euler remplit cette attente dans quatre grands mémoires sur l'équilibre et le mouvement des fluides, qui épuisent tout ce que la théorie complète de l'hydrodynamique peut avoir de plus profond et de plus abstrait.

Cette théorie est infiniment fertile en applications heureuses des principes généraux, et en explications très satisfaisantes de plusieurs phénomènes de la nature. En considérant, par exemple, les dérangemens de l'équilibre de l'air, produits par la différence de sa densité et de sa chaleur, M. Euler explique la cause générale des vents, et particulièrement des moussons ou vents périodiques de l'Inde. En considérant l'équilibre des fluides attirés à un ou à plusieurs centres de forces, il détermine la figure de la terre et l'état d'équilibre des fluides qui l'entourent, ce qui amène l'explication des phénomènes de la marée. Après avoir traité de l'état d'équilibre, il trouve moyen de réduire toute la théorie du mouvement des fluides à deux équations différentielles du second degré, et il applique les principes généraux au mouvement de l'eau dans des vases, dans des pompes, dans des tuyaux d'épaisseur égale et inégale. Les recherches sur le mouvement de l'air le conduisent enfin à la théorie de la propagation du son et à celle de la formation du son des flûtes.

Tels sont les sujets variés et intéressans qu'il vint à bout d'approfondir par sa théorie de l'hydrodynamique. On a si peu écrit sur cette partie épineuse des mathématiques mixtes, et ce que M. Euler y a contribué, est si supérieur à ce peu qu'on a, qu'il serait à souhaiter qu'on le détachât des Commentaires et qu'on en fît un ouvrage séparé, pour le bien de ceux qui veulent étudier à fond cette partie essentielle de la mécanique.

En composant son ouvrage sur la dioptrique, M. Euler avait négligé, dans la théorie des objectifs parfaits, la distance des lentilles dont ils sont composés, ce qui ne peut qu'augmenter les effets de la confusion que ces objectifs devaient détruire; parce que les lentilles ont toujours une certaine épaisseur qu'on ne saurait négliger dans le calcul. Les mémoires sur les objectifs composés et leur application à toutes sortes de lunettes, insérés dans le volume XVIII des Nouveaux Commentaires, sont destinés à suppléer à ce défaut. On y trouve l'exposition des moyens de rendre ces instrumens encore plus courts et leur champ apparent plus grand, avantages qu'il était impossible de donner dans toute leur perfection aux lunettes, avant la dernière simplification des calculs nécessaires. C'est d'après les préceptes renfermés dans ces mémoires, que M. Euler m'a fait calculer, dans la suite, l'instruction pour les artistes opticiens, que l'Académie à fait publier en 1774, et dont une traduction allemande se trouve à la suite de celle de la Dioptrique, faite par M. Klügel à Helmstedt.

Le blâme général de plusieurs caisses mortuaires, établies en Allemagne, et les reproches qu'on faisait aux tontines, d'être trop favorables soit aux entrepreneurs soit aux intéressés, firent penser M. Euler aux moyens d'établir ces sortes d'entreprises sur des principes aussi sûrs que l'imperfection des tables nécrologiques le permet. Ces recherches firent naître les éclaircissemens sur les caisses de veuves etc. qui parurent en 1776. On y trouve tout ce que le calcul des probabilités peut fournir sur ce sujet important.

M. Euler s'était engagé plus d'une fois envers le comte Orlov, de fournir à l'Académie assez de mémoires, pour remplir les Actes jusqu'à vingt ans après sa mort: il était homme à tenir parole. La perte de la vue, les infirmités d'un âge avancé, le grand nombre de ses découvertes [1], n'ont pu ni affaiblir son ardeur du travail, ni détruire son organisation heureuse, ni épuiser son génie fécond. Il a fait présenter, dans l'espace de sept ans, au-delà de soixante-

(1) On eût pu croire que le grand nombre de ses découvertes eût émoussé en lui le sentiment de ce plaisir que cause à l'âme la perception d'une vérité nouvelle, plaisir que le géomètre a l'avantage de goûter peut-être plus souvent que tout autre. M. Euler en était toujours également susceptible, et il aurait voulu que tout le monde le fût. Il était sérieusement fâché de l'air d'indifférence que la modestie me faisait prendre, quand je lui annonçais quelquefois la solution d'un problème ou la démonstration d'un théorème que j'avais réussi à trouver.

dix mémoires par M. Golovine, et près de deux-cents-cinquante autres dont j'avais fait les calculs. Les plus anciens de ces mémoires ont été détachés du reste et forment la collection publiée, dans le cours de cette année, sous le titre d'Opuscules analytiques.

Parmi ce grand nombre de mémoires, il n'y en a pas un seul qui ne renferme quelque nouvelle découverte, ou quelque vue ingénieuse qui pourra y conduire. On y trouve les intégrations les plus heureuses, une multitude d'artifices et de raffinemens de la plus sublime analyse, de profondes recherches sur la nature et les propriétés des nombres, la démonstration ingénieuse de plusieurs théorèmes de Fermat, la solution de quantité de problèmes très difficiles sur l'équilibre et le mouvement des corps solides, flexibles et élastiques, et le dénouement de plusieurs paradoxes apparens. Tout ce que la théorie du mouvement des corps célestes, de leur action mutuelle et de leurs irrégularités a de plus abstrait et de plus épineux, s'y trouve perfectionné, autant que le calcul, manié par les mains du plus grand géomètre, a pu contribuer à cette perfection. Il n'y a pas une branche des sciences mathématiques qui ne lui soit redevable à cet égard.

Tels sont les travaux de M. Euler, tels sont ses titres à l'immortalité: son nom ne périra qu'avec les sciences mêmes. Transmis à la postérite avec les noms illustres de Descartes, Galilée, Leibnitz, Newton, et de tout les grands hommes qui ont honoré l'humanité par leur génie, son nom vivra encore, lorsque ceux de bien des personnages que la frivolité de notre siècle a illustrés, seront ensevelis dans la nuit éternelle de l'oubli.

Peu de savans ont écrit autant que M. Euler; aucun géomètre n'a embrassé tant d'objets à la fois, aucun ne l'a égalé ni pour la multitude ni pour la variété de ses découvertes.

En réfléchissant sur tout le bien que des hommes nés pour étendre les bornes de nos connaissances, peuvent faire à l'humanité; en considérant l'extrême rareté de ces grands talens, à qui la nature paraît avoir réservé le droit d'éclairer le monde: on ne peut s'empêcher de souhaiter, qu'ils fussent exempts de la loi générale que la nature humaine subit tôt ou tard, ou qu'ils poussassent au moins leur carrière loin au-delà du terme ordinaire. Mais enfin, M. Euler en a fourni une bien longue et bien brillante; et on est consolé en partie, en voyant qu'il a été exempt des suites ordinaires d'une application outrée; qu'il a conservé, jusqu'au dernier moment, cette force d'esprit qui l'a distingué toute sa vie, et qu'on découvre jusque dans ses derniers travaux.

Quelques accès de vertiges dont il fut incommodé les premiers jours du mois de septembre passé, ne l'empêchèrent pas de calculer les mouvemens des globes aérostatiques, d'après le peu de faits que les papiers publics en avaient fourni, et il vint à bout d'une intégration très difficile que ce calcul avait exigée. Ces vertiges furent les avant-coureurs de sa mort qui arriva le 7 de septembre. Le même jour il s'entretint, à table, de la nouvelle planète, avec M. Lexell qui était venu le voir; et il nous parla encore d'autres sujets avec sa pénétration ordinaire. Il était même à badiner avec un de ses petits-fils, quand il fut atteint, en prenant le thé, d'un coup d'apoplexie. «Je me meurs», nous dit-il, avant de perdre connaissance, et il termina sa glorieuse vie peu d'heures après, âgé de 76 ans, 5 mois et 3 jours.

Ainsi mourut le doyen de notre Académie, après en avoir été, pendant cinquante-six ans, la gloire et le plus bel ornement: Il a vu cette Académie naître et croître, il l'a vue dépérir et reprendre ses forces alternativement. Et telle a été l'influence de ce membre illustre sur les travaux académiques que, malgré ce qu'il a fait pour elle, pendant son séjour à Berlin, les Commentaires marquent très visiblement l'époque de son départ et celle de son retour, comme si sa présence seule eût été suffisante pour ranimer tout. Il a eu la consolation de voir, avant sa mort, l'aurore des beaux jours que la direction sage et éclairée de son excellence, madame la princesse de Daschkov, fait renaître parmi nous, et sa satisfaction en a été proportionnée à l'attachement qu'il a toujours conservé pour cette Académie.

M. Euler était d'une constitution forte et durable. Après tant de secousses que son physique a dû recevoir du nombre et de la violence de ses maladies, il eût certainement succombé plus tôt aux effets de l'excès du travail, s'il n'eût été né avec une complexion très vigoureuse.

Ses derniers jours ont été tranquilles et sereins. A l'exception de quelques infirmités attachées à un âge avancé, il a joui d'une santé qui le mettait en état de donner à l'étude des momens que la vieillesse se voit communément forcée de donner au repos; et consacrant ainsi à l'étude le reste d'une vie toute entière aux sciences, il a joui de sa gloire, fruit de son génie, de l'estime publique, fruit de ses vertus, et des douceurs qu'il était digne de trouver au sein de sa famille.

Il possedait à un haut degré ce qu'on appelle érudition. Tout ce qui nous est resté des meilleurs écrivains de l'ancienne Rome, il l'avait lu; l'ancienne littérature mathématique lui était parfaitement connue: l'histoire de tous les âges et de toutes les nations se trouvait dans sa tête; il en savait citer les moindres faits sans s'embrouiller. Il savait de la médecine, de la botanique et de la chimie plus qu'on n'attendrait d'un savant qui ne fait pas de ces sciences son étude particulière.

J'ai vu des étrangers qu'attirait chez lui sa célébrité et, plus que sa célébrité, la considération publique, due à des vertus qui n'accompagnent pas toujours le mérite littéraire, je les ai vus le quitter avec une surprise mêlée d'admiration: ils ne conçevaient pas, comment un homme qui, depuis plus d'un demi-siècle, n'avait paru occupé qu'à faire et à publier des découvertes dans la physique et dans les mathématiques, pût avoir conservé tant de connaissances, inutiles pour lui et étrangères à l'objet de ses études. C'était l'effet d'une mémoire heureuse, qui ne perd rien de ce que la lecture lui a confié; et celui qui était en état de réciter, sans interruption, l'Enéide d'un bout à l'autre, et d'indiquer les premiers et les derniers vers de chaque page de son édition, ne pouvait que conserver aussi ce qu'il avait lu dans l'âge des fortes impressions (1).

C'est peut-être de la même source, que provenait en lui le défaut de cette souplesse, qui nous fait contracter insensiblement l'accent de ceux avec qui nous vivons, et perdre celui de notre patrie. M. Euler a toujours conservé la prononciation suisse. Il s'amusait souvent à me rappeller certaines expressions provinciales, certaines inversions propres à notre idiome, ou à se servir, dans ses discours, de mots dont j'avais oublié la signification et l'usage.

Rien n'égale la facilité inconcevable, avec laquelle il pouvait, sans le moindre signe de mécontentement, quitter ses calculs et reprendre le fil de ses profondes méditations, après s'être prêté à la frivolité des conversations ordinaires. L'art de déposer l'air du savant, de déguiser sa supériorité et de se mettre au niveau de tout le monde, est trop rare, pour ne pas faire à M. Euler un mérite de l'avoir possédé. Une humeur toujours égale, une gaieté douce et naturelle, une certaine causticité mêlée de bonhomie, une manière de raconter naïve et plaisante, rendaient sa conversation aussi agréable que recherchée.

Le grand fond de vivacité qu'il a toujours possédé, et sans lequel cette activité d'esprit que nous venons d'admirer, n'aurait pu subsister, l'entrainait quelquefois: il s'échauffait facilement; mais la colère lui passait aussi vite qu'elle s'était enflammée, et il n'a jamais conservé de rancune contre qui que ce soit.

Il était d'une probité, d'une droiture irréprochable. Ennemi juré de toute injustice, s'il en voyait commettre quelque-part, il avait la franchise de la censurer et le courage de l'attaquer ouvertement sans avoir égard à la personne. Des exemples récens de ce que je viens d'avancer, sont encore dans la mémoire de tout le monde.

Il était pénétré de respect pour la religion: sa piété était sincère et sa dévotion pleine de ferveur. Il a rempli, avec la plus grande attention, tous les devoirs du chrétien. Il aimait tout le monde, et s'il a jamais senti les mouvemens de l'indignation, ce ne fut que contre les ennemis de la religion, surtout contre les apôtres déclarés de l'athéisme. Il a pris lui-même la défense de la révélation contre les objections des athées, dans un ouvrage publié à Berlin, en 1747.

(1) Une autre preuve de la force de sa mémoire et de son imagination mérite d'être rapportée ici. Il donnait des leçons d'algèbre et de géométrie à ses petits-fils. L'extraction des racines l'obligeait de leur proposer des nombres qui fussent des puissances: il en fit dans sa tête; et tourmenté d'insomnie, il calcula une nuit les six premières puissances de tous les nombres au-dessous de vingt, et nous les récita, à notre grand étonnement, plusieurs jours après.

Il était bon époux, bon père, bon ami, bon citoyen, et fidèle à toutes les relations de la société. Tout concourt à justifier nos regrets, et à prouver au monde, combien notre douleur de l'avoir perdu est légitime (1).

M. **Euler** s'est marié deux fois. En 1733 il épousa M-lle **Catherine Gsell**, fille d'un peintre suisse, que **Pierre I** avait pris à son service en Hollande, et d'une soeur du célèbre président de **Loën**. Le soin de son ménage l'obligea à se remarier, après la mort de cette épouse, et son choix tomba, en 1776, sur M-lle **Salomé Abigaïl Gsell**, belle-soeur de sa première femme, fille de **Marie Graff** et petite-fille de **Sybille Mérian**, connues l'une et l'autre, par leurs dessins des insectes de Surinam.

De treize enfans qu'il eut de ses premières noces, huit sont morts en bas âge; et de trois fils et deux filles, qui l'ont suivi de Berlin, il n'y a que les fils qui lui ont survécu. L'aîné, qui marche depuis long-temps sur les traces de son illustre père, est justement célèbre, tant par ses propres ouvrages que par la grande part qu'il a eue aux derniers travaux de son père, et par tant de prix remportés dans les Académies de St.-Pétersbourg, de Paris, de Munich et de Göttingen. Le second fils, médecin de la cour de S. M. I. et conseiller de collége, jouit d'une réputation justement méritée par son savoir et par le zèle qu'il met dans l'exercice de son art salutaire. Le cadet, lieutenant-colonel d'artillerie et directeur de la fabrique d'armes à Sisterbek, est connu aux savans par ses observations astronomiques, ayant été du nombre de ceux que l'Académie a envoyés pour observer le passage de Vénus. La fille aînée, morte en 1781, avait épousé M. de **Bell**, major de l'état général; et la cadette s'était mariée avec M. le baron de **Dehlen**, et mourut, sur ses terres dans le duché de Juliers, en 1780. Ces cinq enfans lui ont donné trente-huit petits-enfans, dont vingt-six sont encore en vie.

Je ne connais pas de spectacle plus attendrissant que celui dont j'ai joui tant de fois avec délices, en contemplant ce vieillard vénérable, entouré, comme un patriarche, de sa nombreuse famille, empressée à lui rendre sa vieillesse agréable, et à adoucir ses derniers jours par toutes sortes de soins et d'attentions.

Je tâcherais en vain, Madame et Messieurs, de vous peindre ces scènes touchantes de félicité domestique: plusieurs d'entre vous ont été à portée d'en être, comme moi, témoins oculaires! Vous surtout, Messieurs, qui vous glorifiez de l'avoir eu pour maître (2)! Nous voici au nombre de cinq; y a-t'il un savant, qui puisse se vanter d'avoir vu réunis, dans un même corps, autant de ses disciples? Que ne pouvons nous lui témoigner, à la face du monde, notre tendre et éternelle reconnaissance, et prouver par là, ce que je n'ai pu exprimer que faiblement dans cet éloge: que notre illustre Maître était aussi digne d'admiration par ses rares vertus que par la force étonnante de son génie! Pleurez-le avec les sciences qui lui doivent tant de progrès, avec l'Académie qui n'a jamais fait de perte aussi grande, avec sa famille dont il a été l'honneur et le soutien! Mes larmes se mêleront aux vôtres, et le souvenir des bienfaits que je lui dois en mon particulier, ne s'effacera jamais de ma mémoire.

(1) Il m'est bien doux de pouvoir dire aux lecteurs de cet éloge, que le Roi de Prusse, le Roi de Pologne, le Prince royal de Prusse et le Margrave de Schwedt ont pris part à la perte que l'Académie a faite par la mort de M. **Euler**, et qu'ils ont témoigné, à son fils aîné, leurs regrets, par des lettres de condoléance infiniment honorables au défunt, puisqu'elles rendent justice, dans les termes les plus gracieux, à ses talens comme à ses vertus.

(2) Il y a proprement, à l'Académie, huit mathématiciens, qui ont eu l'avantage de jouir successivement des instructions de M. **Euler**; savoir: MM. **J. A. Euler**, **Kotelnikov**, **Roumovsky**, **Krafft**, **Lexell**, **Inokhodtsov**, **Golovine** et moi; mais trois étaient absens.

O mes chers amis et confrères que j'ai vu verser, à cette apostrophe dictée par le coeur, des larmes d'attendrissement! je n'ai pu que vous serrer la main, après que la douleur m'eût étouffé la voix; mais je ne perdrai jamais le souvenir de cette marque de votre sincère affliction, et je rends ici publiquement justice à votre sensibilité d'ame et à l'amour que vous avez montré, à cette occasion, pour notre cher et incomparable Maître.

INDEX

SYSTÉMATIQUE ET RAISONNÉ

DES

MÉMOIRES ARITHMÉTIQUES

DE

LÉONARD EULER,

CONTENUS

DANS LES DEUX VOLUMES DE CETTE COLLECTION.

PAR

MM. V. BOUNIAKOWSKY ET P. TCHÉBYCHEW.

AVERTISSEMENT.

Sous quelque rapport que l'on considère les diverses recherches sur la Théorie des Nombres, on sera toujours conduit, en définitive, à n'y voir que des applications, plus ou moins directes, de l'Analyse Indéterminée. C'est aussi la manière de voir de Legendre qui ne sépare point ces deux parties, et les regarde comme ne faisant qu'une seule et même branche de l'analyse algébrique. En partant de ce point de vue, et prenant en considération la variété infinie des équations indéterminées, on découvre un champ immense dans les spéculations sur les nombres. Pour procéder méthodiquement dans les nombreuses recherches de ce genre, la première question qui se présente naturellement est de savoir si, parmi toutes ces équations, il ne s'en trouve pas quelques unes qui méritent une étude particulière et approfondie sous le rapport de leur utilité et de leur application aux questions les plus générales et les plus intéressantes de l'Arithmétique transcendante. Or, c'est précisément ce qui arrive, et l'on sait fort bien, que la propriété que les nombres possèdent de satisfaire à certaines classes d'équations indéterminées, est caractérisée, dans les recherches numériques, par différentes dénominations telles que *divisibilité*, *congruence*, *forme quadratique* etc. Toutes ces propriétés servent de base aux différentes doctrines de la science des nombres. Ainsi, la résolution des équations indéterminées, de forme très variée, repose presqu'en entier sur les notions fondamentales, relatives à la divisibilité, aux congruences et aux formes quadratiques.

D'après ce qui vient d'être dit, il est très naturel de partager un traité sur la Théorie des Nombres en deux parties, dont la première doit contenir tout ce qui est relatif aux généralités de la science, telles que les recherches sur la divisibilité de diverses formules, la théorie des congruences, celle des formes quadratiques etc., et la seconde, les applications de tous ces principes à la résolution des équations indéterminées de différentes formes, ou à la solution des problèmes qui se réduisent à de telles équations. Les subdivisions à établir, pour être parfaitement systématiques, exigeraient beaucoup plus de peine, et laisseraient peut-être, malgré tous les soins, à désirer sous plusieurs rapports, vu la grande variété et l'hétérogénéité, du moins apparente, des questions que l'on a fait entrer dans la Théorie des Nombres. Aussi, un programme détaillé et bien raisonné de cette science, serait-il un travail très méritoire.

En examinant avec soin les nombreux mémoires d'Euler sur l'arithmétique transcendante, et en les classant conformément aux idées, en partie émises plus haut, on parvient à former un ensemble qui, sauf quelques légères lacunes, présente un traité suffisamment complet sur la science des nombres en général, et même fort étendu par rapport à plusieurs de ses doctrines. Dans la rédaction de l'Index systématique, que nous donnons ci-après, nous nous sommes conformés à ce qui vient d'être dit relativement à la division de la science en deux parties. Seulement, pour faciliter la recherche des mémoires d'Euler, nous avons subdivisé la seconde partie, c'est-à-dire les applications des principes généraux à l'analyse indéterminée ou à l'analyse de Diophante, en deux sections: l'une qui traite de la décomposition des nombres en sommes de différentes formes, et l'autre qui contient l'analyse de Diophante proprement dite. De cette manière, l'Index se trouve divisé en trois sections, auxquelles nous avons joint un appendice sous le titre de *Mélanges*, qui, au reste, ne contient que cinq mémoires. Nous avons cru devoir les mettre à part par la raison, que les questions dont ils traitent, se rapportent moins directement à la théorie des nombres.

Ainsi, pour nous résumer, voici en termes généraux le contenu de l'Index:

Première Section. *Divisibilité des nombres.* On y a réuni tout ce qui concerne la décomposition des nombres en facteurs, les différentes recherches sur les nombres premiers, sur les sommes des diviseurs, les nombres amiables, sur la divisibilité de différentes formules, sur la théorie des restes et sur celle des résidus quadratiques.

Seconde Section. *Décomposition des nombres en sommes de différentes formes.* On trouvera dans cette section tous les mémoires relatifs à la décomposition des nombres en carrés, en nombres triangulaires, et en général, tout ce qui se rapporte à la partition des nombres. Dans les mémoires de cette section le nombre à décomposer est généralement *donné*, tandis-que dans les problèmes de la troisième section tous les nombres, le plus souvent, sont *indéterminés*, et c'est en cela que nous faisons consister la différence entre ces deux sections.

Ttroisième Section. *Analyse de Diophante.* Cette section, la plus étendue de toutes, contient les mémoires relatifs à la résolution de différentes équations indéterminées, données immédiatement, ou bien déduites des conditions du problème. Pour réduire la recherche des mémoires sur cette matière à la plus grande simplicité, nous avons jugé que la classification la plus avantageuse était de les ranger dans l'ordre du *nombre des équations simultanées à résoudre*, et non dans celui du *nombre des indéterminées* ou des *degrés des équations.*

Mélanges. Mémoires qui se rapportent plus ou moins directement à la théorie des nombres.

Pour ce qui regarde les subdivisions des trois sections, elles ont été établies aussi systématiquement que possible, et sans jamais perdre de vue la condition essentielle pour un Index, celle de rendre la recherche des mémoires aussi facile qu'on peut le désirer. On en jugera par la lecture attentive de la distribution des matières dans l'Index, distribution que nous rapportons ici:

Section Première.

Divisibilité des nombres.

a) Sur les nombres entiers, eu égard à leur décomposition en facteurs. Tables des nombres premiers. Totalité des nombres premiers à un entier donné et plus petits que lui. Sur les sommes des diviseurs des nombres. Nombres amiables.

b) Divisibilité de différentes formules.

c) Théorie des restes et des résidus quadratiques.

Remarques sur la section première.

Section Seconde.

Décomposition des nombres en sommes de différentes formes.

a) Décomposition des nombres en carrés, en nombres triangulaires et en termes proportionnels à des carrés.

b) Partition des nombres.

Remarques sur la section seconde.

Section Troisième.

Analyse de Diophante.

a) Détermination de deux ou de plusieurs indéterminées, données par une seule équation. — Equations impossibles.

b) Détermination de plusieurs indéterminées, données par deux équations.

c) Détermination de plusieurs indéterminées, données par trois équations.

d Détermination de plusieurs indéterminées, données par quatre équations.

e) Détermination de plusieurs indéterminées, données par plus de quatre équations.

f) Problèmes indéterminés qui conduisent à plus d'équations que d'inconnues.

Remarques sur la section troisième.

Mélanges.

Par cette distribution des matières, nous croyons avoir atteint jusqu'à un certain point deux buts:

1) celui d'avoir donné un programme systématique pour étudier la théorie des nombres dans les nombreux mémoires d'Euler, et

2) d'avoir présenté un Index qui servira non-seulement à trouver sans peine tous ses mémoires relatifs à une théorie quelconque de la science des nombres, mais encore à donner une idée générale du contenu de chacun de ses écrits.

L'Index acquerrait un haut degré d'intérêt, si on l'accompagnait, ou si on le faisait suivre de notes comparatives sur les diverses méthodes, employées dans les mémoires d'Euler, et sur celles qui ont été proposées plus tard pour les mêmes questions. Dans un examen de cette nature, il se présenterait une foule de rapprochements et d'observations curieuses. On pourrait aussi faire entrer dans ces remarques, ou notes additionelles, des renvois raisonnés à la *Correspondance mathématique et physique* d'Euler *et de* Goldbach, ouvrage qui contient tant de vues ingénieuses et remarquables

sur la science des nombres. Enfin, une appréciation motivée de l'importance respective des différents travaux d'Euler sur cette branche de l'analyse, compléterait parfaitement l'appendice dont nous parlons. Mais un tel travail demanderait beaucoup de temps, et ne pourrait être entrepris que par un Géomètre versé à fond dans l'analyse numérique.

Entrons actuellement dans quelques explications sur la forme de l'Index et sur la manière de l'employer. Et d'abord, on observera que les titres originaux des mémoires sont accompagnés de numéros en chiffres arabes qui suivent l'ordre naturel; immédiatement après le numéro arabe vient un autre, en caractères romains, qui indique la place que le mémoire occupe dans l'ouvrage. De plus, à la fin de chaque titre, est donnée l'Indication du tome et de la page où se trouve l'écrit que l'on veut consulter. Les remarques qui suivent chaque section sont également numérotées, et, pour ne pas confondre ces nouveaux numéros avec ceux que portent les mémoires dans l'Index, on les a fait précéder du signe §. En regard du titre original de chaque mémoire, se trouve, à la droite, un sommaire de son contenu; ceci nous a paru d'autant plus nécessaire, qu'un grand nombre de ces titres ne peuvent donner aucune idée des recherches exposées dans les pièces correspondantes.

Supposons maintenant que l'on veuille faire usage de l'Index pour trouver les travaux d'Euler sur une doctrine quelconque de la théorie des nombres. Par la nature de cette doctrine, on décidera de suite à laquelle des trois sections elle appartient; puis, parcourant les titres des subdivisions, relatives à cette section, on trouvera sans peine la subdivision cherchée, et par suite, aussi tous les mémoires que l'on avait en vue. Il pourra arriver que, dans les sommaires des mémoires trouvés, il y ait encore des renvois; il faudra absolument consulter tous ces renvois, après quoi on sera à même de se former une idée générale, aussi complète qu'il est nécessaire, pour un simple Index, des travaux d'Euler sur la matière en question. Enfin, on parcourra les *Remarques* qui se trouvent placées à la fin de la section consultée, afin de voir si quelques points relatifs à la doctrine dont il s'agit ne sont point entrés, comme parties secondaires, dans d'autres pièces, dont l'objet principal était différent. Vu la grande analogie qui existe entre les sections seconde et troisième, comme nous l'avons dit plus haut, il sera bon de consulter l'une et l'autre, toutes les fois qu'il s'agira d'une question de l'analyse indéterminée qui, par sa nature, donnerait lieu à quelque incertitude.

Eclaircissons ce qui vient d'être expliqué d'une manière générale, par un exemple particulier. Proposons nous de trouver le mémoire d'Euler qui traite de la question de *trouver cinq nombres tels que le produit de deux quelconques de ces nombres, augmenté de l'unité, fasse un carré*(1). Comme ce problème appartient, sans le moindre doute, à l'analyse de Diophante proprement dite, il faudra chercher le mémoire dans la section troisième; de plus, on observera qu'il conduit à *dix* équations indéterminées. En parcourant les subdivisions de la troisième section, on s'arrête à la subdivision *e*) qui porte pour titre: *Détermination de plusieurs indéterminées, données par plus de quatre équations.* Sur les trois mémoires que contient cette subdivision, aucun ne traite de la question dont il s'agit. Il faudra donc consulter les *Remarques sur la subdivision e) de la Section troisième.* En effet, on y

(1) Legendre, en donnant la solution de ce problème d'après Euler (Théorie des nombres, troisième édition, T. 2 page 142), dit l'avoir extrait de la Correspondance d'Euler avec Lagrange, et renvoie aux manuscrits de Lagrange déposés à la bibliothèque de l'Institut. Quant au mémoire que nous allons trouver, il n'en fait point mention.

trouve que le *sixième* paragraphe du mémoire XLV (N. 19 de l'Index), portant pour titre *Miscellanea analytica*, contient la solution du problème dont nous parlons. Si l'on désire connaître le contenu des autres paragraphes de ce même écrit, on cherchera le N. 19 de l'Index et l'on trouvera ce qui suit:

«Cet écrit est composé de 6 paragraphes, dont le premier contient la démonstration du théorème de Waring, ou autrement de Wilson, relatif à la divisibilité de la formule $1.2.3\ldots(p-1)+1$ par p, quand p est premier. Les paragraphes 2, 3, 4 et 6 se rapportent à l'analyse de Diophante, et il en est fait mention dans les *Remarques* à la Section troisième. Quant au paragraphe 5 qui traite la question de trouver les sommes des puissances de α, β, γ...., quand le développement de $(1+\alpha x)(1+\beta x)(1+\gamma x)\ldots.$ est donné, il est étranger à la théorie des nombres.»

On saura donc déjà ce que contiennent les paragraphes *premier*, *cinquième* et *sixième*. Pour les paragraphes *deuxième*, *troisième* et *quatrième*, on consultera les renvois dont il vient d'être question dans la citation, et l'on trouvera:

Deuxième Paragraphe. *Trouver quatre nombres tels que le produit de deux quelconques de ces nombres, augmenté de l'unité, se réduise toujours à un carré.*

Troisième Paragraphe. Méthode pour réduire la formule $\left(\frac{x^2+1}{x}\right)^2+\left(\frac{y^2+1}{y}\right)^2$ à un carré.

Quatrième Paragraphe. Résolution des deux équations indéterminées simultanées $x+y=u^2$, $x^2+y^2=v^4$.

De cette manière le lecteur se formera une idée nette du contenu des *Miscellanea analytica*, et pourra, au besoin, recourir au mémoire même qui, d'après l'Index, se trouve inséré au II Tome, page 44.

Prenons encore, pour exemple, le problème II, inséré dans la théorie des nombres de Legendre (T. 2, page 144). Le géomètre français, après en avoir rapporté une solution numérique, tirée de la correspondance d'Euler avec Lagrange, citée plus haut, s'exprime en ces termes: «L'analyse de ce problème n'a point été publiée, et il est fort à désirer qu'elle le soit, si on peut la trouver parmi les manuscrits de l'auteur, non encore imprimés, car on voit qu'il serait fort difficile de la restituer.» Or, par l'énoncé de la question, on verra de suite qu'elle se rapporte à la II Section, *subdivision f)*, portant pour titre: *problèmes indéterminés qui conduisent à plus d'équations que d'inconnues.* En consultant l'Index, on trouve que le *troisième problème* du premier mémoire qui entre dans cette subdivision (N. 86 de l'Index), est précisément celui dont il s'agit, et que, de plus, la solution de cette question, ainsi que celle des deux autres, mentionnées sous la même rubrique, est fondée sur des considérations relatives à la doctrine de la transformation des coordonnées, qui est d'un intérêt majeur pour la géométrie analytique. Il paraît donc certain que Legendre n'a pas eu connaissance de ce mémoire, ni par conséquent de la méthode ingénieuse d'Euler pour résoudre la question citée. Le mémoire dont nous parlons porte le numéro XXX dans l'ouvrage, et se trouve dans le Tome I à la page 427.

Outre les 88 mémoires publiés et les 5 inédits qui se trouvent classés dans cet Index, le présent ouvrage contient encore un traité inédit, d'une certaine étendue, sur la doctrine des nombres

(*Tractatus de numerorum doctrina*, T. II, p. 503) et 4 numéros sous le titre *Additamenta tomi secundi*; ces fragments intéressants sont tirés d'une riche collection de feuillets détachés et de pièces manuscrites d'Euler, dont plusieurs, malheureusement, se trouvent incomplètes.

Le traité dont nous parlons est composé de *seize* chapitres; en voici le contenu:

Chapitre I *Sur la composition des nombres.*

Chapitre II. *Sur les diviseurs des nombres.*

Chapitre III. *Sur les sommes des diviseurs des nombres.*

Chapitre IV. *Sur les nombres premiers et non-premiers entr'eux.*

Chapitre V. *Résidus de la division.*

Chapitre VI. *Des résidus qui naissent de la division des termes d'une progression arithmétique.*

Chapitre VII. *Des résidus qui naissent de la division des termes d'une progression géométrique.*

Chapitre VIII. *Sur les puissances des nombres dont la division par des nombres premiers donne l'unité pour reste.*

Chapitre IX. *Sur les diviseurs des nombres de la forme* $a^n \pm b^n$.

Chapitre X. *Sur les résidus quadratiques par rapport à des nombres premiers.*

Chapitre XI. *Sur les résidus cubiques par rapport à des nombres premiers.*

Chapitre XII. *Sur les résidus biquadratiques par rapport à des nombres premiers.*

Chapitre XIII. *Sur les résidus qui naissent de la division des cinquièmes puissances par des nombres premiers.*

Chapitre XIV. *Des résidus quadratiques par rapport à des nombres composés.*

Chapitre XV. *Sur les diviseurs des nombres de la forme* $x^2 + y^2$.

Chapitre XVI. *Sur les diviseurs des nombres de la forme* $x^2 + 2y^2$.

Les fragments dont il a été question plus haut, sont les suivants:

1) *De numeris amicabilibus* (T. II, p. 627) qui contient quelques recherches analytiques sur les nombres amiables.

2) *De numeris amicabilibus* (T. II, p. 637) qui contient une table de *trente paires* de nombres amiables, dont *quatre* ne sont point entrées dans le mémoire X (T. I, p. 102), portant le même titre que ce fragment. Les quatre paires de nombres amiables dont nous parlons sont:

$$2^2.5.131 \quad \text{et} \quad 2^2.17.43,$$
$$2^2.5.251 \quad \text{et} \quad 2^2.13.107,$$
$$2^4.19.8563 \quad \text{et} \quad 2^4.83.2039,$$
$$2^5.47.2609 \quad \text{et} \quad 2^5.11.59.173.$$

3) *Découverte d'une loi tout extraordinaire des nombres, par rapport à la somme de leurs diviseurs.* (T. II, p. 639). C'est le premier travail d'Euler contenant l'énoncé de la loi remarquable que suivent les sommes des diviseurs des nombres, et qui est exprimée, comme on le sait, par la formule

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) - \ldots$$

Dans cet écrit, il présente cette loi simplement comme un résultat de l'induction, et en observant même que sa démonstration lui paraît très difficile. Ce n'est que dans le mémoire XVI (T. I, p. 234) qu'il l'établit sur des considérations rigoureuses. M. C.-G.-J. Jacobi, dans ses *Mathematische Werke* (T. 1. p. 345), donne une démonstration élémentaire, très élégante, de cette formule remarquable.

4) (T. II, p. 648). Cette pièce n'est qu'un petit fragment d'un mémoire qui, par les numéros des paragraphes existants, paraît avoir été fort étendu. Les §§ 49, 50 et 51 contiennent la résolution de la question suivante: *Trouver un triangle dans lequel les trois droites, menées de chacun de ses sommets aux milieux des côtés opposés, s'expriment rationellement.* Ce même problème est traité dans les mémoires XXXVI, LXXI, LXIX et LXXXVII (NN. 72, 73, 74 et 75 de l'Index.)

Dans les §§ 52, 53, 54 et 55, Euler résoud la question de *trouver trois nombres carrés tels, que la somme de deux quelconques d'entr'eux soit toujours un carré.* On voit que ce problème est une extension de celui de trouver un triangle rectangle rationel. Sa signification géométrique revient à *construire un parallélépipède rectangle en nombres rationels, avec la condition que les diagonales de chacune de ses faces s'expriment rationellement.*

Nous terminerons ces éclaircissements en présentant une table qui établit la correspondance des numéros que les mémoires portent dans l'ouvrage avec les numéros de l'Index. Cette table offrira le moyen de trouver immédiatement, en consultant l'Index, le contenu d'un mémoire quelconque, ce qui, fort souvent, peut être très utile.

Correspondance des numéros des mémoires dans l'ouvrage avec leurs numéros dans l'Index.

I	18	XX	26	XXXIX	46	LVIII	63	LXXVII	64
II	43	XXI	34	XL	48	LIX	3	LXXVIII	59
III	25	XXII	44	XLI	47	LX	9	LXXIX	58
IV	16	XXIII	41	XLII	24	LXI	4	LXXX	65
V	52	XXIV	89	XLIII	40	LXII	8	LXXXI	60
VI	20	XXV	10	XLIV	42	LXIII	5	LXXXII	79
VII	17	XXVI	2	XLV	19	LXIV	6	LXXXIII	54
VIII	70	XXVII	38	XLVI	77	LXV	45	LXXXIV	68
IX	37	XXVIII	92	XLVII	1	LXVI	7	LXXXV	50
X	15	XXIX	78	XLVIII	39	LXVII	23	LXXXVI	61
XI	12	XXX	86	XLIX	91	LXVIII	55	LXXXVII	75
XII	31	XXXI	69	L	14	LXIX	74	LXXXVIII	57
XIII	33	XXXII	80	LI	90	LXX	88	LXXXIX	(*)
XIV	51	XXXIII	53	LII	11	LXXI	73	XC	83
XV	32	XXXIV	29	LIII	36	LXXII	62	XCI	93
XVI	13	XXXV	30	LIV	21	LXXIII	81	XCII	87
XVII	71	XXXVI	72	LV	22	LXXIV	82	XCIII	76
XVIII	85	XXXVII	28	LVI	49	LXXV	67	XCIV	84
XIX	27	XXXVIII	35	LVII	56	LXXVI	66		

(*) *Tractatus de numerorum doctrina* (Avertissement de l'Index, T. I, p. LVIII.)

INDEX SYSTÉMATIQUE

DES MÉMOIRES DE L. EULER RELATIFS A LA THÉORIE DES NOMBRES.

Section première.

DIVISIBILITÉ DES NOMBRES.

a) *Sur les nombres entiers, eu égard à leur décomposition en facteurs. Tables des nombres premiers. Totalité des nombres, premiers à un entier donné et plus petits que lui. Sur les sommes des diviseurs des nombres. Nombres amiables.*

1. XLVII. *De tabula numerorum primorum, usque ad millionem et ultra continuanda; in qua simul omnium numerorum non primorum minimi divisores exprimantur.* (*T.* II, *p.* 64.)

Sur la construction des tables des nombres premiers et des plus petits diviseurs des nombres composés, depuis 1 jusqu'à 1000000, et au-delà.

2. XXVI. *Quomodo numeri praemagni sint explorandi, utrum sint primi, nec ne?* (*T.* I, *p.* 379.)

Recherches sur les nombres de la forme $4m+1$, en tant qu'ils sont premiers ou composés.

3. LIX. *De variis modis numeros praegrandes examinandi, utrum sint primi, nec ne?* (*T.* II, *p.* 198.)

4. LXI. *Methodus generalior numeros quosvis satis grandes perscrutandi, utrum sint primi, nec ne?* (*T.* II, *p.* 220.)

5. LXIII. *De formulis speciei* mxx+nyy *ad numeros primos explorandos idoneis, earumque mirabilibus proprietatibus.* (*T.* II, *p.* 249.)

6. LXIV. *Illustratio paradoxi circa progressionem numerorum idoneorum, sive congruorum.* (*T.* II, *p.* 261.)

7. LXVI. *Extrait d'une lettre à M.* Béguelin. (*T.* II, *p.* 270.)

Les mémoires 3, 4, 5, 6 et 7 contiennent: 1) des recherches sur la divisibilité des nombres quand on les décompose en sommes de la forme $x^2+\lambda y^2$, $\alpha x^2+\beta y^2$; 2) la détermination des expressions de cette forme, ayant la propriété de ne fournir qu'une solution à l'équation

$$\alpha x^2+\beta y^2=N,$$

dans le seul cas où N est premier; 3) les valeurs du produit $\alpha\beta$ pour lesquelles l'équation $\alpha x^2+\beta y^2=N$ jouit de cette propriété; 4) l'examen de ces valeurs de $\alpha\beta$, désignées sous la dénomination de *numeri idonei* (*nombres convenables*) (1); on prouve en même temps que leur nombre n'est que de 65, et que le plus grand d'entr'eux est égal à 1848.

8. LXII. *Utrum hic numerus: 1000009 sit primus, nec ne, inquiritur.* (*T.* II, *p.* 243.)

Examen du nombre 1000009; on arrive à la conclusion que ce nombre est composé, et que son plus petit diviseur est 293.

(1) C'est ainsi qu'Euler les appelle lui même en français dans l'*Extrait d'une lettre à M.* Béguelin, N. LXVI. ci-contre.

9. LX. *Facillima methodus plurimos numeros primos praemagnos inveniendi.* (*T.* II, *p.* 215.)

Détermination d'une multitude de nombres premiers par l'exclusion des valeurs de a qui réduisent la formule $232a^2+1$ à un nombre composé.

10. XXV. *De numeris primis valde magnis.* (*T.* I, *p.* 356.)

Ce mémoire commence par l'observation que la formule $2^{2^n}+1$ qui, suivant une assertion de Fermat, ne devrait contenir que des nombres premiers, se réduit, pour $n=5$, à un nombre composé, dont le plus petit diviseur est égal à 641. Euler fait voir ensuite, qu'il n'existe aucune fonction algébrique entière, propre à n'exprimer que des nombres premiers. Recherche des valeurs de a, pour lesquelles la formule a^2+1 est divisible par un nombre premier donné de la forme $4n+1$.

Viennent ensuite les tables suivantes:

1) Une table dont la première colonne contient, par ordre de grandeur, tous les nombres premiers de la forme $4n+1$, jusqu'à 1997, décomposés en deux carrés, et la seconde les valeurs de a qui rendent la somme a^2+1 divisible par ces mêmes nombres.
2) Une table, moins étendue, contenant les valeurs de a propres à rendre la somme a^2+1 divisible par des puissances des nombres premiers de la forme $4n+1$.
3) Quatre tables qui contiennent les valeurs de a propres à réduire les quatre formules

$$a^2+1, \quad \frac{a^2+1}{2}, \quad \frac{a^2+1}{5} \quad \text{et} \quad \frac{a^2+1}{10}$$

à des nombres premiers.
4) Une table des diviseurs de la formule a^2+1, depuis $a=1$ jusqu'à $a=1500$, qui fournit une multitude de nombres premiers de grandeur considérable.

11. LII. *Speculationes circa quasdam insignes proprietates numerorum.* (*T.* II, *p.* 127.)

Déduction de la formule pour trouver, combien il y a de nombres plus petits qu'un nombre donné, et premiers avec lui. (Voyez aussi, à ce sujet, le N. 26 de l'Index).

Découverte d'une loi tout extraordinaire des nombres, par rapport à la somme de leurs diviseurs. (*T.* II, *p.* 639.)

12. XI. *Observatio de summis divisorum.* (*T.* I, *p.* 146.)

13. XVI. *Demonstratio theorematis circa ordinem in summis divisorum observatum.* (*T.* I, *p.* 234.)

Ces trois mémoires traitent de la détermination des sommes des diviseurs des nombres. Pour le premier de ces mémoires, voyez l'*Avertissement* (p. LVIII). Le second contient une table de ces sommes pour tous les nombres jusqu'à 100. Enfin, dans le troisième, on trouve la démonstration rigoureuse de la loi remarquable qui lie entr'elles les sommes des diviseurs de différents nombres.

14. L. *De mirabilibus proprietatibus numerorum pentagonalium.* (*T.* II, *p.* 105.)

Différentes recherches sur le développement du produit infini $(1-x)(1-x^2)(1-x^3)(1-x^4)\ldots$ par rapport à la somme des diviseurs d'un nombre. — Diverses propriétés des nombres pentagonaux.

15. X. *De numeris amicabilibus.* (*T.* I, *p.* 102.)

Ce mémoire contient des recherches très étendues sur les *nombres amiables*, c'est-à-dire sur deux nombres tels, que chacun d'eux soit égal à la somme des parties aliquotes de l'autre, en excluant toute fois de cette somme le nombre lui même. — On trouve aussi dans ce mémoire 1) une table des sommes des diviseurs de différentes puissances de tous les nombres premiers, inférieurs à 1000. Ces sommes de diviseurs sont présentées sous forme de produits de facteurs simples. 2) 61 paires de nombres amiables.

De numeris amicabilibus. (*T.* II, *p.* 627.)

Voyez l'*Avertissement* (p. LVIII.)

De numeris amicabilibus. (*T.* II, *p.* 637.)

Voyez l'*Avertissement* (p. LVIII).

b) *Divisibilité de différentes formules.*

16. IV. *Theorematum quorundam ad numeros primos spectantium demonstratio.* (*T.* I, *p.* 21.)

Démonstration du théorème de Fermat relatif à la divisibilité de $a^{p-1}-1$ par p, quand p est premier, et a premier à p. (Voyez le N. 27 de l'Inde x).

17. VII. *Theoremata circa divisores numerorum.* (*T.* I, *p.* 50.)

Sur les diviseurs des nombres de la forme

$$(a+b)^p-a^p-b^p,\ (a+b)^p-a-b,\ a^p-a,$$
$$a^{p-1}-b^{p-1},\ a^{2^m}+b^{2^m}.$$

18. I. *Observationes de theoremate quodam Fermatiano, aliisque ad numeros primos spectantibus.* (*T.* I, *p.* 1.)

Sur les diviseurs des nombres de la forme

$$a^n\pm1,\ a^{n^{m-1}(n-1)}-1,\ 3^n\pm1,\ 3^n\pm2^n.$$

Additamentum ad annum 1772. *Extrait d'une lettre à M.* Bernoulli, *concernant le mémoire imprimé parmi ceux de* 1771 *p.* 318. (*T.* I, *p.* 584.)

Critères pour juger laquelle des deux formules

$$10^{\frac{p-1}{2}}-1,\quad \text{ou}\quad 10^{\frac{p-1}{2}}+1,$$

est divisible par p, p étant un nombre premier. En outre cette lettre contient deux remarques intéressantes:

1) que le plus grand nombre premier connu est

$$2^{31}-1=2147483647;$$

2) que les quarante premiers termes de la formule

$$41-x+x^2$$

sont tous des nombres premiers.

19. XLV. *Miscellanea analytica.* (*T.* II, *p.* 44.)

Cet écrit est composé de 6 paragraphes, dont le premier contient la démonstration du théorème de Waring, ou autrement de Wilson, relatif à la divisibilité de la formule $1.2.3\ldots(p-1)+1$ par p, quand p est premier.

Les paragraphes 2, 3, 4 et 6 se rapportent à l'analyse de Diophante, et il en est fait mention dans les *Remarques* à la *Section troisième*. Quant au paragraphe 5, qui traite la question de trouver les sommes des puissances α, β, $\gamma\ldots$, quand le développement de $(1+\alpha x)(1+\beta x)(1+\gamma x)\ldots$ est donné, il est étranger à la théorie des nombres.

20. VI. *Theoremata circa divisores numerorum in hac forma* paa ± qbb *contentorum.* (*T.* I, *p.* 35.)

21. LIV. *De insigni promotione scientiae numerorum.* (*T.* II, *p.* 140.)

22. LV. *Novae demonstrationes circa divisores numerorum formae* xx + nyy. (*T.* II, *p.* 159.)

23. LXVII. *De divisoribus numerorum in forma* mxx + nyy *contentorum.* (*T.* II, *p.* 272.)

NN. 20 à 23. Sur les diviseurs des nombres de la forme $mx^2 + ny^2$. Ces quatre mémoires renferment des recherches très étendues sur cette matière et un grand nombre de théorèmes qui s'y rapportent. Les mémoires LV et LXVII contiennent en outre des tables d'un usage utile dans cette théorie.

24. XLII. *De quibusdam eximiis proprietatibus circa divisores potestatum occurrentibus.* (*T.* II, *p.* 1.)

Sur les diviseurs des nombres de la forme $fa^r + g$. Le supplément à ce mémoire contient des recherches sur les restes que l'on obtient en divisant des nombres carrés par des entiers de forme donnée; on y trouve aussi des propositions sur les diviseurs de quelques formes quadratiques. Ce supplément se rapporte donc en partie à la subdivision *c*) ci-dessous.

c) *Théorie des restes et des résidus quadratiques.*

25. III. *Solutio problematis arithmetici de inveniendo numero, qui per datos numeros divisus, relinquat data residua.* (*T.* I, *p.* 11.)

Détermination d'un nombre qui, divisé par un entier donné, produit un reste également donné. Cette question se réduit à la résolution d'une équation indéterminée du premier degré à deux inconnues. Exemples numériques.

26. XX. *Theoremata arithmetica nova methodo demonstrata.* (*T.* I, *p.* 274.)

Sur les restes provenant de la division des termes successifs d'une progression arithmétique et géométrique. De là on déduit la formule qui sert à trouver combien il y a de nombres plus petits qu'un nombre donné, et premiers avec lui; (N. 11 de l'Index). Extension du théorème de **Fermat**, démontré dans le numéro 16 de l'Index, au cas d'un diviseur composé quelconque.

27. XIX. *Theoremata circa residua ex divisione potestatum relicta.* (*T.* I, *p.* 260.)

Recherches sur les propriétés de la série des restes que l'on obtient en divisant par un nombre premier les termes successifs de la progression géométrique

$$1,\ a,\ a^2,\ a^3 \ldots\ldots$$

Ces considérations conduisent à une démonstration du théorème de **Fermat**, exposé dans le N. 16 de l'Index.

28. XXXVII. *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.* (*T.* I, *p.* 516.)

Diverses propositions sur les restes provenant de la division des termes de la progression géométrique

$$1,\ a,\ a^2,\ a^3 \ldots\ldots$$

par un nombre premier. Cas, où cette série comprend tous les nombres inférieurs au nombre premier donné; la base *a*, qui satisfait à cette condition, s'appelle *racine primitive*. Totalité des racines primitives appartenant à un nombre premier donné. Table de ces racines pour les

onze nombres premiers 3, 5, 7, 11, 13, 17, 19, 23, 31 et 37. Généralisation du théorème de Fermat dont il est aussi question dans le N. 26 de l'Index. — Sur les diviseurs de quelques formes quadratiques.

29. XXXIV. *Observationes circa divisionem quadratorum per numeros primos.* (*T.* 1, *p.* 477.)

30. XXXV. *Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta.* (*T.* 1, *p.* 487.)

Ces deux mémoires contiennent une théorie détaillée des résidus quadratiques et des indices; on y trouve aussi des tables fort utiles pour cette matière.

REMARQUES SUR LA SECTION PREMIÈRE.

A la subdivision *a*) se rapportent:

§ 1. La fin du mémoire XII (N. 31 de l'Index) qui traite de la question de savoir, si un nombre donné, de la forme $4m+1$, est ou non premier. On arrive à ce but en décidant, si ce nombre est décomposable en deux carrés, et cela d'une seule manière.

§ 2. La fin du mémoire XIII (N. 33).

A la subdivision *b*):

§ 3. Les chapitres I, II, III et IV du *Tractatus de numerorum doctrina*, T. II, p. 503. (Voyez l'*Avertissement.*)

§ 4. Le commencement du mémoire XV (N. 32 de l'Index), qui contient quelques propositions sur la divisibilité des formules binomes.

§ 5. Quelques passages des mémoires XIII (N. 33), XXI (N. 34), XXXVII (N. 28) et XXXVIII (N. 35), qui contiennent des observations sur les diviseurs des formes quadratiques.

A la subdivision *c*):

§ 6. Les chapitres IX, XV et XVI du *Tractatus de numerorum doctrina*, T. II, p. 503. (Voyez l'*Avertissement.*)

§ 7. Une partie du supplément au mémoire XLII (N. 24 de l'Index) et le mémoire LV (N. 22) en tant qu'il y est question des résidus quadratiques.

§ 8. La partie du mémoire XXXVIII (N. 35) dans laquelle il est question de la divisibilité de la formule $\lambda x^2+\mu y^2+\nu z^2$ par un nombre premier.

§ 9. Les chapitres V, VI, VII, VIII, X, XI, XII, XIII et XIV du *Tractatus de numerorum doctrina*, T. II, p. 503. (Voyez l'*Avertissement*).

§ 10. Le mémoire XV (N. 32) par l'analyse qui y est employée.

Section seconde.

DÉCOMPOSITION DES NOMBRES EN SOMMES DE DIFFÉRENTES FORMES.

a) *Décomposition des nombres en carrés, en nombres triangulaires et en termes proportionnels à des carrés.*

31. XII. *De numeris, qui sunt aggregata duorum quadratorum.* (*T.* 1, *p.* 155.)

Décomposition d'un nombre en deux carrés. Démonstration de la proposition de Fermat relative à ce que tout nombre premier de la forme $4n+1$ est décomposable en deux carrés, et cela d'une seule manière. La fin du mémoire se rapporte à la distinction des nombres de la forme $4n+1$, en tant qu'ils sont premiers ou composés.

(Voyez § 1 des *Remarques sur la Section première*).

32. XV. *Demonstratio theorematis Fermatiani, omnem numerum primum formae* 4n+1 *esse summam duorum quadratorum.* (*T.* I, *p.* 210.)

Décomposition d'un nombre premier de la forme $4n+1$ en deux carrés, et d'un nombre quelconque en quatre carrés, fondée sur la théorie des résidus quadratiques.

33. XIII. *Specimen de usu observationum in mathesi pura.* (*T.* I, *p.* 174.)

Représentation des nombres par la forme $2x^2+y^2$, fondée sur les propriétés des diviseurs de la formule $2a^2+b^2$. Application de ces principes à la distinction des nombres premiers.

34. XXI. *Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur.* (*T* I, *p.* 287.)

Représentation des nombres par la forme $3x^2+y^2$, fondée sur les propriétés des diviseurs de la formule $3a^2+b^2$. Le commencement du mémoire se rapporte à la *Section troisième, subdivision a*).

35. XXXVIII. *Novae demonstrationes circa resolutionem numerorum in quadrata.* (*T.* I, *p.* 538.)

Représentation des nombres par les formes

x^2+y^2, x^2+2y^2, x^2+3y^2, $x^2+y^2+z^2+u^2$,

fondée sur les propriétés des diviseurs de ces mêmes formules. Les sommes dont il est question fournissent des exemples de *fonctions semblables* qui, étant multipliées entre elles, donnent des produits semblables. Recherches sur la manière de rendre la somme

$$\lambda x^2+\mu y^2+\nu z^2$$

divisible par un nombre premier donné qui ne divise aucun des trois coefficients λ, μ, ν. (Voyez le § 8 des *Remarques sur la première Section.*)

36. LIII. *De inductione ad plenam certitudinem evehenda.* (*T.* II, *p.* 134.)

Décomposition d'un nombre en quatre carrés et en trois triangulaires, fondée sur une proposition, non démontrée, et à laquelle on parvient par voie d'induction. Cette proposition consiste en ce que *tout nombre pairement-impair est décomposable en deux nombres premiers de la forme* 4n+1.

b) *Partition des nombres.*

37. IX. *De partitione numerorum.* (*T.* I, *p.* 73.)

Représentation des nombres par des sommes de différentes formes, fondée sur le développement des produits composés d'une infinité de facteurs. Ce mémoire contient une table, assez étendue, indiquant de combien de manières un nombre donné n peut être formé par l'addition des nombres de la série 1, 2, 3....m.

38. XXVII. *De partitione numerorum in partes tam numero quam specie datas.* (*T.* I, *p.* 391.)

Recherches du même genre que dans le mémoire précédent.

39. XLVIII. *Considerationes super theoremate Fermatiano de resolutione numerorum in numeros polygonales.* (*T.* II, *p.* 92.)

Considérations sur le théorème de Fermat, relatif à la décomposition des nombres en nombres polygonaux. L'auteur s'appuie dans ces recherches sur les développements que l'on obtient en élevant des polynomes convenables à de certaines puissances.

40. XLIII. *Proposita quacunque progressione ab unitate incipiente, quaeritur, quot ejus terminos ad minimum addi oporteat, ut omnes numeri producantur?* (*T.* II, *p.* 27.)

Sur le nombre *minimum* des termes de la série

$$\frac{n+a}{1}, \quad \frac{(n+1)(n+2a)}{1.2}, \quad \frac{(n+1)(n+2)(n+3a)}{1.2.3}.$$

et en général

$$\frac{(n+1)(n+2)(n+3)\ldots\ldots(n+ka)}{1.2.3\ldots k},$$

dont on puisse former par l'addition un nombre entier quelconque.

REMARQUES SUR LA SECTION SECONDE.

A la subdivision *a*) se rapportent en partie:

§ 11. Les mémoires LIX (N. 3 de l'Index), LXI (N. 4), LXIII (N. 5), LXVI (N. 7) et LX (N. 9), et en général toutes les questions de l'analyse de Diophante.

A la subdivision *b*):

§ 12. Les mémoires XI (N. 12 de l'Index) et XVI (N. 13).

Section troisième.

ANALYSE DE DIOPHANTE.

a) *Détermination de deux ou de plusieurs indéterminées, données par une seule équation. Equations impossibles.*

41. XXIII. *De usu novi algorithmi in problemate Pelliano solvendo.* (*T.* I, *p.* 316.)

42. XLIV. *Nova subsidia pro resolutione formulae*

$$axx + 1 = yy.$$

(*T.* II, *p.* 35.)

Ces deux mémoires traitent de la résolution de l'équation indéterminée de Pell: $ax^2+1=y^2$. En outre, l'Auteur a accompagné le premier de ces mémoires de deux tables, fort utiles dans ce problème. La première contient le développement de tous les nombres, non-carrés, au-dessous de 121, en fractions continues; la seconde donne les solutions *minima* de l'équation $ax^2+1=y^2$, pour toutes les valeurs de a, non-carrées, au-dessous de 100.

43. II. *De solutione problematum Diophanteorum per numeros integros.* (*T.* I, *p.* 4.)

44. XXII. *De resolutione formularum quadraticarum indeterminatarum per numeros integros.* (*T.* I, *p.* 297.)

NN. 43. 44. Résolution de l'équation indéterminée du second degré $ax^2+bx+c=y^2$ en nombres rationnels et en nombres entiers.

45. LXV. *Regula facilis problemata Diophantea per numeros integros expedite resolvendi* (*T.* II, *p.* 263.).

Résolution de l'équation indéterminée du second degré

$$\alpha x^2+\beta x+\gamma=\zeta y^2+\eta y+\vartheta.$$

L'Auteur applique sa méthode à la solution de plusieurs questions particulières, telles que:

1) *Trouver tous les nombres triangulaires qui soient en même temps des carrés.*

2) *Trouver tous les nombres carrés tels, qu'en les diminuant de l'unité, on obtienne des nombres triangulaires.*

3) *Trouver les nombres triangulaires qui, étant triplés, donnent également des nombres triangulaires.*

Ces questions conduisent évidemment à la résolution des trois équations indéterminées suivantes:

1) $\frac{x^2+x}{2}=y^2$, 2) $x^2-1=\frac{y^2+y}{2}$, 3) $3\cdot\frac{x^2+x}{2}=\frac{y^2+y}{2}$.

46. XXXIX. *Resolutio aequationis* $Ax^2+2Bxy+Cy^2+2Dx-2Ey+F=0$ *per numeros tam rationales, quam integros.* (*T.* I, *p.* 549.)

Résolution de l'équation complète du second degré à deux indéterminées, tant en nombres rationnels qu'en nombres entiers.

47. XLI. *De resolutione irrationalium per fractiones continuas, ubi simul nova quaedam et singularis species minimi exponitur.* (*T.* I, *p.* 570.)

Dans ce mémoire, qui traite de la résolution générale de l'équation indéterminée du second degré

$$Ax^2+2Bxy+Cy^2+Dx+Ey+F=0,$$

Euler s'attache particulièrement à la discussion du cas le plus difficile, c'est-à-dire de celui où l'équation dont il s'agit, après avoir été ramenée à la forme

$$Ax^2+2Bxy+Cy^2=H,$$

admet une infinité de solutions, ce qui a lieu quand

$$B^2-AC>0.$$

La méthode employée dans ce mémoire est fondée sur la considération des fractions continues, et conduit à des résultats curieux sur le *minimum* de la formule mx^2-ny^2 en nombres entiers. Nous observerons aussi que l'analyse dont Lagrange a fait usage en traitant le problème de Pell, a beaucoup d'analogie avec celle d'Euler.

48. XL. *De criteriis aequationis* $fxx+gyy=hzz$, *utrum ea resolutionem admittat, nec ne?* (*T.* I, *p.* 556.)

Caractères pour reconnaître si l'équation indéterminée du second degré $fx^2+gy^2=hz^2$ est résoluble ou non.

49. LVI. *De singulari genere quaestionum Diophantearum et methodo maxime recondita eas resolvendi.* (*T.* II, *p.* 174.)

Ce mémoire a pour but la résolution de la question suivante: la représentation du nombre N par la forme a^2+nb^2 étant donnée, trouver:

1) les représentations des puissances N^2, N^3, N^4.... par la même forme x^2+ny^2;

2) les valeurs *minima* des indéterminées soit de x, soit de y.

50. LXXXV. *De resolutione hujus aequationis:* $0=a+bx+cy+dx^2+exy+fy^2+gx^2y+hxy^2+ix^2y^2$ *per numeros rationales.* (*T.* II, *p.* 467.)

Résolution de l'équation indéterminée

$$0=a+bx+cy+dx^2+exy+fy^2+gx^2y+hxy^2+ix^2y^2$$

en nombres rationnels.

51. XIV. *Solutio generalis quorundam problematum Diophanteorum, quae vulgo nonnisi solutiones speciales admittere videntur.* (*T.* I, *p.* 193.)

Résolution des équations indéterminées:

$$x^2+y^2=z^2,\quad x^3+y^3+z^3=v^3,\quad x^3+y^3=z^2.$$

Ce mémoire contient une table des nombres de la forme m^2+3n^2, inférieurs à 1000.

52. V. *Theorematum quorundam arithmeticorum demonstrationes.* (*T.* I, *p.* 24.)

Démonstration de l'impossibilité des deux équations: $x^4 \pm y^4 = z^2$, en nombres rationnels. Même conclusion par rapport aux équations $2x^4 \pm 2y^4 = z^2$, sauf le cas évident de $x = y$, et aux formules

$$mx^4 \pm m^2y^4 = z^2, \quad 2mx^4 \pm 2m^2y^4 = z^2.$$

Aucun nombre triangulaire, l'unité exceptée, ne peut être égal à un bi-carré. La formule $x^4 + 2y^4$ ne peut se réduire à un carré, sauf le cas $y = 0$. Si la formule $a^4 + kb^4$ ne peut devenir un carré, la même impossibilité aura lieu par rapport à la formule $2k\alpha\beta^2y^4 - 2\alpha^2\beta x^4$. Impossibilité de l'équation $x^3 + 1 = z^2$ en nombres rationnels, sauf les cas $x = 0$ et $x = 2$.

53. XXXIII. *Observationes circa bina biquadrata, quorum summam in duo alia biquadrata resolvere liceat.* (*T.* I, *p.* 473.)

54. LXXXIII. *Dilucidationes circa binas summas duorum biquadratorum inter se aequales.* (*T.* II, *p.* 450.)

NN 53. 54. Résolution de l'équation indéterminée

$$x^4 + y^4 = u^4 + v^4$$

en nombres rationnels, et par suite en nombres entiers.

55. LXVIII. *Resolutio formulae Diophanteae*

$$ab(maa + nbb) = cd(mcc + ndd)$$

per numeros rationales. (*T.* II, *p.* 281.)

Résolution de l'équation indéterminée

$$ab(ma^2 + nb^2) = cd(mc^2 + nd^2)$$

en nombres rationnels. La résolution de cette équation conduit immédiatement à la décomposition de la somme de deux bi-carrés en une somme semblable. Ce même problème est traité dans les deux mémoires précédents (N. 53 et N. 54.)

56. LVII. *De casibus, quibus hanc formulam*

$$x^4 + kxxyy + y^4$$

ad quadratum reducere licet. (*T.* II, *p.* 183.)

57. LXXXVIII. *De casibus, quibus formulam*

$$x^4 \pm mx^2y^2 + y^4$$

ad quadratum reducere licet. (*T.* II, *p.* 492.)

NN. 56. 57. Recherches sur les cas dans lesquels la formule $x^4 \pm kx^2y^2 + y^4$ peut se réduire à un carré.

58. LXXIX. *De insigni promotione analysis Diophanteae.* (*T.* II, *p.* 418.)

Sur la résolution des équations indéterminées:

$$a^2x^4 + 2bx^3y + cx^2y^2 + 2bdxy^3 + d^2y^4 = u^2,$$

$$(ax^2 + 2bx + c)^2 - 4mx^2 = u^2,$$

$$\alpha x^4 \pm \beta y^4 = u^2.$$

59. LXXVIII. *Resolutio facilis quaestionis difficillimae, qua haec formula maxime generalis:*

$$v^2z^2(ax^2 + by^2)^2 + \Delta x^2y^2(av^2 + bz^2)^2$$

ad quadratum reduci postulatur. (*T.* II, *p.* 414.)

Résolution de l'équation indéterminée

$$v^2z^2(ax^2 + by^2)^2 + \Delta x^2y^2(av^2 + bz^2)^2 = u^2.$$

60. LXXXI. *Investigatio binorum numerorum formae*

$$xy(x^4 - y^4),$$

quorum productum, sive quotus sit quadratum. (*T.* II, *p.* 438.)

Ce mémoire contient la solution de la question suivante: *Trouver deux nombres de la forme* $xy(x^4 - y^4)$ *dont le produit et le quotient soient tous deux des carrés*, ou, autrement, *trouver les solutions de l'équation indéterminée:*

$$xy(x^4 - y^4) \cdot x'y'(x'^4 - y'^4) = u^2,$$

car, si cette équation est satisfaite, le quotient des deux

nombres $xy(x^4 - y^4)$ et $x'y'(x'^4 - y'^4)$ sera nécessairement un nombre carré.

61. LXXXVI. *Methodus nova et facilis formulas cubicas et biquadraticas ad quadratum reducendi.* (*T.* II, *p.* 474.)

Détermination des valeurs de x qui réduisent l'expression biquadratique

$$(1) \quad A+Bx+Cx^2+Dx^3+Ex^4$$

à un carré complet, lorsque le développement de cette même expression (1) en une somme de la forme

$$(2) \quad (a+bx+cx^2)^2+(d+ex+fx^2)(g+hx+ix^2)$$

est connu. Et réciproquement, réduction de l'expression (1) à la forme (2), quand on connaît les valeurs de x qui rendent la formule (1) égale à un carré. Recherches analogues pour la formule cubique $A+Bx+Cx^2+Dx^3$.

62. LXXII. *De casibus quibusdam maxime memorabilibus in analysi indeterminata, ubi imprimis insignis usus calculi angulorum in analysi Diophantea ostenditur.* (*T.* II, *p.* 366.)

Euler s'occupe dans ce mémoire de la résolution de chacune des deux équations

$$x^4+y^4+z^4-2x^2y^2-2x^2z^2-2y^2z^2+2x^2v^2+2y^2v^2+2z^2v^2+v^4=0$$

$$x^4+y^4+z^4+v^4-2x^2y^2-2x^2z^2-2x^2v^2-2y^2z^2-2y^2v^2-2z^2v^2=0.$$

Ces équations méritent une attention particulière par la propriété qu'elles ont de pouvoir être présentées sous des formes très remarquables; ainsi, la première d'entr'elles, est susceptible de prendre les *sept* formes suivantes:

I. $x^2y^2-z^2v^2=\frac{1}{4}(x^2+y^2-z^2+v^2)^2$

II. $x^2z^2-y^2v^2=\frac{1}{4}(x^2+z^2-y^2+v^2)^2$

III. $y^2z^2-x^2v^2=\frac{1}{4}(y^2+z^2-x^2+v^2)^2$

IV. $x^2y^2-v^2(x^2+y^2)=\frac{1}{4}(x^2+y^2-z^2-v^2)^2$

V. $x^2z^2-v^2(x^2+z^2)=\frac{1}{4}(x^2+z^2-y^2-v^2)^2$

VI. $y^2z^2-v^2(y^2+z^2)=\frac{1}{4}(y^2+z^2-x^2-v^2)^2$

VII. $x^2y^2+x^2z^2+y^2z^2=\frac{1}{4}(x^2+y^2+z^2+v^2)^2$.

En se fondant sur les formules I et II, Euler fait voir que les indéterminées x, y, z, v doivent satisfaire aux conditions

$$\frac{x^2}{v^2}=\frac{(p^2+r^2)(q^2+s^2)}{4prqs}=\square, \qquad \frac{y^2}{z^2}=\frac{qs(p^2+r^2)}{pr(q^2+s^2)}=\square,$$

dont il fait usage pour déterminer p, q, r, s. Il propose deux méthodes pour cette détermination: l'une, fondée sur des considérations arithmétiques, et l'autre, sur l'emploi des fonctions trigonométriques.

Une analyse analogue conduit Euler à la résolution de la seconde équation, c'est-à-dire

$$x^4+y^4+z^4+v^4-2x^2y^2-2x^2z^2-2x^2v^2-2y^2z^2-2y^2v^2-2z^2v^2=0.$$

Il commence par observer qu'elle peut être présentée sous les *huit* formes suivantes:

I. $2\sqrt{(x^2y^2+z^2v^2)}=x^2+y^2-z^2-v^2$,

II. $2\sqrt{(x^2z^2+y^2v^2)}=x^2+z^2-y^2-v^2$,

III. $2\sqrt{(x^2v^2+y^2z^2)}=x^2+v^2-y^2-z^2$,

IV. $2\sqrt{(x^2y^2+x^2z^2+y^2z^2)}=x^2+y^2+z^2-v^2$,

V. $2\sqrt{(x^2y^2+x^2v^2+y^2v^2)}=x^2+y^2+v^2-z^2$,

VI. $2\sqrt{(x^2z^2+x^2v^2+z^2v^2)}=x^2+z^2+v^2-y^2$,

VII. $2\sqrt{(y^2z^2+y^2v^2+z^2v^2)}=y^2+z^2+v^2-x^2$

VIII. $2\sqrt{(x^2y^2+x^2z^2+x^2v^2+y^2z^2+y^2v^2+z^2v^2)}=x^2+y^2+z^2+v^2$.

Pour cette seconde équation, on trouve

$$\frac{x^2}{v^2}=\frac{(p^2-r^2)(q^2-s^2)}{4prqs},\qquad \frac{y^2}{z^2}=\frac{qs(p^2-r^2)}{pr(q^2-s^2)},$$

et la question se réduit à trouver les valeurs de p, q, r, s satisfaisant à la condition

$$\frac{(p^2-r^2)(q^2-s^2)}{prqs}=\square,$$

objet pour lequel Euler présente également deux méthodes.

b) *Détermination de plusieurs indéterminées, données par deux équations.*

63. LVIII. *De novo genere quaestionum arithmeticarum, pro quibus solvendis certa methodus adhuc desideratur.* (*T.* II, *p.* 190.)

Discussion des valeurs de N pour lesquelles la résolution simultanée des deux équations

$$A^2+B^2=u^2,\quad A^2+NB^2=v^2,$$

est possible. Le problème se ramène

1) à la détermination des valeurs fractionnaires de α qui réduisent la formule

$$(\alpha x^2\pm1)(\alpha y^2\pm1)$$

à un nombre entier, et

2) à la recherche des valeurs rationnelles de x et y, propres à réduire à un entier le produit

$$(x^2\pm1)(y^2\pm1).$$

64. LXXVII. *De binis formulis speciei*

$$xx+myy \quad et \quad xx+nyy$$

inter se concordibus et discordibus. (*T.* II, *p.* 406.)

Sur les valeurs simultanées de m et n propres à rendre résolubles les deux équations indéterminées

$$x^2+my^2=u^2 \quad \text{et} \quad x^2+ny^2=v^2.$$

65. LXXX. *Solutio problematis difficillimi, quo hae duae formulae:* $a^2x^2+b^2y^2$ *et* $b^2x^2+a^2y^2$ *quadrata reddi debent.* (*T.* II, *p.* 425.)

Solution des deux équations indéterminées simultanées

$$a^2x^2+b^2y^2=u^2 \quad \text{et} \quad b^2x^2+a^2y^2=v^2.$$

La fin du mémoire, à partir du § 30, est consacrée à la solution du problème suivant:

Trouver quatre nombres carrés tels, que chacune des trois sommes que l'on obtient en ajoutant le produit de deux d'entr'eux au produit des deux autres, soit un carré complet.

En d'autres termes, si l'on représente par a^2, b^2, c^2, d^2 les quatre nombres cherchés, on aura à résoudre en nombres entiers les trois équations simultanées

$$a^2b^2+c^2d^2=u^2,$$
$$a^2c^2+b^2d^2=v^2,$$
$$a^2d^2+b^2c^2=w^2.$$

Cette dernière question, comme on le voit, se rapporte à la subdivision suivante c).

66. LXXVI. *Solutio problematis Fermatiani de duobus numeris, quorum summa sit quadratum, quadratorum vero summa biquadratum, ad mentem ill.* La Grange *adornata.* (*T.* II, *p.* 403.)

67. LXXV. *De tribus pluribusve numeris inveniendis, quorum summa sit quadratum, quadratorum vero summa biquadratum.* (*T.* II, *p.* 397.)

NN. 66. 67. Le premier de ces mémoires contient la solution d'un problème de Fermat qui consiste à trouver deux nombres tels, que leur somme soit égale à un carré, et la somme de leurs carrés, à un bi-carré.

Dans le second mémoire la solution est étendue au cas de trois ou de plusieurs nombres satisfaisant aux mêmes conditions, ou, en d'autres termes, on y donne la solution des équations indéterminées

$$\begin{cases} x+y+z=u^2 \\ x^2+y^2+z^2=v^4 \end{cases}$$
$$\begin{cases} x+y+z+t+\ldots=u^2 \\ x^2+y^2+z^2+t^2+\ldots=v^4. \end{cases}$$

68. LXXXIV. *De tribus numeris quadratis, quorum tam summa, quam summa productorum ex binis sit quadratum.* (*T.* II, *p.* 457.)

Résolution des deux équations indéterminées simultanées

$$x^2+y^2+z^2=u^2,$$
$$x^2y^2+x^2z^2+y^2z^2=v^2.$$

69. XXXI. *Solutio quorundam problematum Diophanteorum.* (*T.* I, *p.* 444.)

Ce mémoire contient la solution de trois questions sur l'analyse indéterminée:

1) La résolution des deux équations simultanées:

$$(x^2+y^2)(t^2x^2+u^2y^2)=U^2$$
$$(x^2+y^2)(u^2x^2+t^2y^2)=V^2$$

avec plusieurs solutions numériques.

2) La résolution de l'équation indéterminée

$$(t^2x^2+u^2y^2)(u^2x^2+t^2y^2)=V^2.$$

3) La résolution des deux équations simultanées

$$t^2x^2+u^2y^2=U^2,$$
$$t^2y^2+u^2x^2=V^2.$$

La seconde question se rapporte, comme on le voit, à la subdivision a) de cette *troisième Section.*

c) *Détermination de plusieurs indéterminées, données par trois équations.*

70. VIII. *Solutio problematis difficillimi a* Fermatio *propositi.* (*T.* I, *p.* 62.)

Le problème, résolu dans ce mémoire, consiste à trouver un triangle rectangle en nombres rationnels et tel que chacun de ses cathètes étant diminué de l'aire du triangle, produise un nombre carré. Si l'on représente donc générale

ment par $\frac{2x}{z}$ et $\frac{y}{z}$ les deux cathètes, l'hypoténuse sera $\frac{\sqrt{(4x^2+y^2)}}{z}$ et l'aire du triangle $\frac{xy}{z^2}$, et la question se réduira à la résolution des trois équations indéterminées simultanées:

$$2xz-xy=u^2,$$
$$yz-xy=v^2,$$
$$4x^2+y^2=w^2.$$

71. XVII. *Solutio problematis de investigatione trium numerorum, quorum tam summa, quam productum, nec non summa productorum ex binis, sint numeri quadrati.* (*T.* I, *p.* 239.)

Résolution des trois équations indéterminées simultanées:

$$x+y+z=u^2,$$
$$xy+xz+yz=v^2,$$
$$xyz=w^2.$$

72. XXXVI. *Solutio problematis de inveniendo triangulo, in quo rectae ex singulis angulis latera opposita bisecantes sint rationales.* (*T.* I, *p.* 507.)

73. LXXI. *Solutio facilior problematis* Diophantei *circa triangulum, in quo rectae ex angulis latera opposita bisecantes rationaliter exprimantur.* (*T.* II, *p.* 362.)

74. LXIX. *Investigatio trianguli, in quo distantiae angulorum ab ejus centro gravitatis rationaliter exprimantur.* (*T.* II, *p.* 294.)

75. LXXXVII. *Problème de géométrie, résolu par l'analyse de* Diophante. (*T.* II, *p.* 488.)

Les §§ 49, 50 et 51 du fragment portant le N. 4 (T. II, p. 649.) Voyez l'*Avertissement* p. LIX.

Ces cinq pièces traitent de la résolution du problème suivant:

Trouver un triangle en nombres rationnels de manière à ce que les trois droites qui joignent les sommets des trois angles avec les milieux des côtés opposés, soient également rationnelles.

Si l'on représente par $2a$, $2b$, $2c$ les côtés du triangle cherché, et par f, g, h les trois droites dont il vient d'être question dans l'énoncé, le problème se réduira à résoudre les trois équations indéterminées simultanées:

$$2b^2+2c^2-a^2=f^2,$$
$$2c^2+2a^2-b^2=g^2,$$
$$2a^2+2b^2-c^2=h^2.$$

Ce même problème peut aussi être évidemment énoncé de la manière suivante:

Trouver un triangle en nombres rationnels tel, que les distances de ses trois sommets à son centre de gravité, soient également rationnelles.

76. XCIII. *Recherches sur le problème de trois nombres carrés tels, que la somme de deux quelconques, moins le troisième, fasse un nombre carré* (*). (*T.* II. *p.* 603, inédit.)

Résolution des trois équations indéterminées simultanées

$y^2+z^2-x^2=p^2$, $x^2+z^2-y^2=q^2$, $x^2+y^2-z^2=r^2$.

Euler, après avoir ramené ce problème à la résolution de l'équation unique

$$a^4+b^4-4a^2b^2=r^2,$$

propose quatre méthodes pour en trouver une infinité de solutions. On trouve aussi dans ce mémoire la démonstration de la proposition que tous les nombres premiers $8n+1$ et $8n+3$ sont toujours de la forme a^2+2b^2, et cela d'une seule manière.

(*) Voyez *Prooemium*, p. XXI.

Les §§ 52, 53, 54 et 55 du fragment portant le N. 4. (T. II, p. 650.)

Les paragraphes cités contiennent la résolution de la question suivante: *trouver trois nombres carrés tels, que la somme de deux quelconques d'entr'eux soit toujours un carré.* (Voyez l'*Avertissement* p. LIX).

d) *Détermination de plusieurs indéterminées, données par quatre équations.*

77. XLVI. *Problema Diophanteum singulare.* (*T.* II, *p.* 53.)

Résolution des quatre équations indéterminées simultanées:

$$xy+xz=t^2,\quad xy+yz=u^2,$$
$$xy-xz=v^2,\quad xy-yz=w^2.$$

78. XXIX. *Solutio problematis, quo duo quaeruntur numeri, quorum productum tam summa, quam differentia eorum, sive auctum sive minutum, fiat quadratum.* (*T.* I, *p.* 414.)

Résolution des quatre équations indéterminées simultanées

$$xy+x+y=t^2,\qquad xy-x+y=v^2,$$
$$xy-x-y=u^2,\qquad xy+x-y=w^2.$$

79. LXXXII. *De binis numeris, quorum summa sive aucta, sive minuta tam unius quam alterius quadrato, producat quadrata.* (*T.* II, *p.* 447.)

Résolution des quatre équations indéterminées simultanées

$$z(x+y)+x^2=t^2,\qquad z(x+y)-x^2=v^2,$$
$$z(x+y)+y^2=u^2,\qquad z(x+y)-y^2=w^2.$$

80. XXXII. *Problematis cujusdam Diophantei evolutio.* (*T.* I, *p.* 450.)

Le premier problème, traité dans ce mémoire, conduit à la résolution des quatre équations indéterminées simultanées

$$x+y+z+s=t^2,\quad xy+xz+xs+yz+ys+zs=u^2,$$
$$xyz+xys+xzs+yzs=v^2,\quad xyzs=w^2,$$

qui, elles mêmes, donnent lieu à examiner quelques autres formules assez remarquables.

La seconde question se rapporte, par le nombre des équations indéterminées auxquelles elle conduit, à la subdivision *e*). Elle consiste à trouver des nombres rationnels p, q, r, s, etc. tels, qu'en représentant par S leur somme, chacun des produits

$$p(S-p),\quad q(S-q),\quad r(S-r),\quad s(S-s)\quad \text{etc.}$$

soit égal à un carré.

Enfin, dans l'appendice à ce mémoire, se rapportant également à la subdivision *e*), il s'agit de trouver des nombres carrés

$$A^2,\quad B^2,\quad C^2,\quad D^2\quad \text{etc.}$$

de manière qu'en supposant

$$S=A^2+B^2+C^2+D^2+\ldots,$$

toutes les différences

$$S-A^2,\quad S-B^2,\quad S-C^2,\quad S-D^2\quad \text{etc.}$$

soient des nombres carrés.

81. LXXIII. *Investigatio quadrilateri, in quo singulorum angulorum sinus datam inter se teneant rationem;*

Dans ce mémoire l'auteur commence par donner la solution du problème suivant: *Trouver un quadrilatère tel,*

ubi artificia prorsus singularia in analysi Diophantea occurrunt. (*T.* II, *p.* 380.)

que les sinus de ses quatre angles soient entr'eux dans une raison rationnelle donnée. L'analyse employée par **Euler** dans cette question le conduit immédiatement à la solution d'un problème de **Diophante**, dont voici l'énoncé: *Les quatre carrés* a^2, b^2, c^2, d^2 *étant donnés, trouver deux nombres* z *et* v *tels, que chacune des quatre formules*

$$z - a^2v,\quad z - b^2v,\quad z - c^2v,\quad z - d^2v$$

se réduise à un carré.

L'auteur termine son mémoire par la recherche de quatre nombres entiers a, b, c, d tels, qu'ayant

$$a > b > c > d,$$

et de plus $b+c > a+d$, les trois formules

$$ab - cd,\quad ac - bd,\quad bc - ad$$

se réduisent à des carrés. Ce dernier problème conduisant à *trois* équations indéterminées simultanées, se rapporte à la subdivision précédente *c*).

e) *Détermination de plusieurs indéterminées, données par plus de quatre équations.*

82. LXXIV. *Solutio succincta et elegans problematis, quo quaeruntur tres numeri tales, ut tam summae quam differentiae binorum sint quadrata.* (*T.* II, *p.* 392.)

Résolution des six équations indéterminées simultanées

$$x+y=p^2,\quad x+z=q^2,\quad y+z=r^2,$$
$$x-y=u^2,\quad x-z=v^2,\quad y-z=w^2.$$

83. XC. *Considerationes circa analysin Diophanteam.* (*T.* II, *p.* 576, inédit.)

Ce mémoire contient la résolution des quatre problèmes suivants:

1) *Trouver trois nombres* v, x, y *tels, que chacune des trois sommes*

$$vx+v+x,\quad vy+v+y,\quad xy+x+y$$

se réduise à un carré.

Cette question, comme on le voit, se rapporte à la subdivision *c*) de cette *troisième Section.*

2) *Trouver quatre nombres* A, B, C, D *tels, que chacune des six différences*

$$AB-1,\quad AC-1,\quad AD-1,\quad BC-1,\quad BD-1,\quad CD-1$$

soit un carré.

3) *Trouver quatre nombres* A, B, C, D *tels, que chacune des six sommes*

$$AB+n,\quad AC+n,\quad AD+n,\quad BC+n,\quad BD+n,\quad CD+n$$

se réduise à un carré.

4) *Trouver quatre nombres* A, B, C, D *tels, que chacun des six doubles produits*

$$AB,\quad AC,\quad AD,\quad BC,\quad BD,\quad CD,$$

augmenté de la somme A+B+C+D *de ces mêmes nombres, produise un carré.*

Après ce problème, **Euler** donne une solution numérique d'une question analogue, dans laquelle, au lieu des six sommes de la forme

$$AB+A+B+C+D,$$

il s'agit de réduire à un carré les six différences

$$AB-A-B-C-D,\quad AC-A-B-C-D \text{ etc.}$$

84\. XCIV. *Recherches sur le problème de quatre nombres positifs et en proportion arithmétique tels, que la somme de deux quelconques soit toujours un nombre carré* (1). (*T.* II, *p.* 617, inédit.)

Dans ce mémoire, très important par l'analyse qui y est employée, **Euler** résoud les six équations indéterminées simultanées

$$A+B=p^2,\quad A+C=q^2,\quad A+D=r^2,$$
$$B+C=r^2,\quad B+D=s^2,\quad C+D=t^2.$$

en nombres positifs et entiers.

La solution du problème est fondée sur l'observation, que ces six équations se ramènent aux deux suivantes:

$$2r^2=p^2+t^2=q^2+s^2$$

avec les conditions

$$p<t,\quad q<s,\quad r^2<p^2+q^2.$$

85\. XVIII. *De problematibus indeterminatis, quae videntur plus quam determinata.* (*T.* I, *p.* 245.) (2)

Résolution des huit équations indéterminées simultanées

$$xy+z=p^2,\quad xy+x+y=u^2,$$
$$xz+y=q^2,\quad xz+x+z=v^2,$$
$$yz+x=r^2,\quad yz+y+z=w^2,$$
$$xy+xz+yz=s^2,$$
$$xy+xz+yz+x+y+z=t^2.$$

Cette question conduit l'auteur à l'examen d'un grand nombre de formules qui, sous certaines conditions, représentent des nombres carrés. En même temps, ces considérations lui fournissent le moyen de résoudre plusieurs problèmes de l'analyse de **Diophante**.

f) *Problèmes indéterminés qui conduisent à plus d'équations que d'inconnues.*

86\. XXX. *Problema algebraicum ob affectiones prorsus singulares memorabile.* (*T.* I, *p.* 427.)

Ce mémoire contient la solution des trois problèmes que voici:

1) Trouver *neuf* nombres qui, étant disposés dans un carré comme ci-dessous

$$\begin{matrix} A & B & C \\ D & E & F \\ G & H & J \end{matrix}$$

satisfassent aux *douze* conditions suivantes:

(1) Voyez *Prooemium*, p. XXI.

(2) Quoique **Euler** regarde la question, traitée dans ce mémoire, comme appartenant à la classe de celles qui fournissent plus d'équations que d'indéterminées, nous avons cru devoir la faire entrer dans la subdivision e), parce que, à notre avis, chaque nouvelle équation introduit dans le problème une nouvelle indéterminée.

$$A^2+D^2+G^2=1, \quad AB+DE+GH=0,$$
$$B^2+E^2+H^2=1, \quad AC+DF+GJ=0,$$
$$C^2+F^2+J^2=1, \quad BC+EF+HJ=0,$$
$$A^2+B^2+C^2=1, \quad AD+BE+CF=0,$$
$$D^2+E^2+F^2=1, \quad AG+BH+CJ=0,$$
$$G^2+H^2+J^2=1, \quad DG+EH+FJ=0.$$

2) Trouver 25 nombres A, B, C, D.... qui, étant disposés de façon à former le carré que voici

$$\begin{matrix} A & B & C & D & E \\ F & G & H & J & K \\ L & M & N & O & P \\ Q & R & S & T & U \\ V & W & X & Y & Z \end{matrix}$$

satisfassent aux 30 conditions suivantes: *a*) que la somme des carrés des nombres soit égale à l'unité dans chacune des cinq lignes horizontales, ainsi que dans chacune des cinq lignes verticales, ce qui fait 10 conditions; *b*) que la somme des produits deux-à-deux tels que

$$AF+BG+CH+DJ+EK$$

soit nulle par rapport à deux lignes horizontales quelconques, aussi bien qu'à l'égard de deux lignes verticales arbitraires, ce qui fait 20 conditions; en tout 30.

3) Trouver 16 nombres, inscrits dans un carré,

$$\begin{matrix} A & B & C & D \\ E & F & G & H \\ J & K & L & M \\ N & O & P & Q \end{matrix}$$

tels que *a*) la somme des carrés dans chacune des lignes horizontales, verticales et de plus dans les deux diagonales soit la même, ce qui fait 10 conditions; *b*) que la somme des produits deux-à-deux soit nulle, tant par rapport aux nombres formant deux lignes horizontales quelconques, qu'à l'égard de ceux qui forment deux lignes verticales arbitraires, ce qui fait 12 conditions; en tout 22 conditions.

Les solutions de ces trois problèmes sont fondées sur des considérations très ingénieuses relatives à la doctrine de la transformation des coordonnées; par cela même ce mémoire est d'un intérêt majeur pour la géométrie analytique.

87. XCII. *De quadratis magicis.* (*T.* II, *p.* 593, inédit.)

L'auteur donne dans ce mémoire une construction des carrés magiques à 9, 16, 25 et 36 cellules, fondée sur un moyen particulier, consistant dans la superposition de deux systèmes de nombres, choisis d'une certaine manière.

88. LXX. *Recherches sur une nouvelle espèce de carrés magiques.* (*T.* II, *p.* 302)

Ce mémoire, comme le dit Euler lui même, a été écrit au sujet d'un problème fort curieux, qui a exercé, pendant

quelque temps, la sagacité de plusieurs personnes. Il était question d'une assemblée de 36 officiers de 6 différents grades et de 6 régiments différents, qu'il s'agissait de ranger dans un carré, de manière que sur chaque ligne tant horizontale que verticale, il se trouvât six officiers tant de différents grades que de régiments différents. Or, après un grand nombre d'essais, on a été obligé de reconnaître qu'un tel arrangement était absolument impossible, sans qu'on ait pu cependant en donner une démonstration rigoureuse.

Il résulte des recherches contenues dans ce mémoire, que la question est impossible toutes les fois que le côté du carré, c'est-à-dire le nombre des régiments et par conséquent aussi celui des grades, est *impairement pair*. A la verité, cette impossibilité ne se trouve pas établie en toute rigueur mathématique; mais elle est pourvue d'un tel degré de probabilité par les raisonnements d'Euler, que le doute devient presque impossible. Au contraire, quand le côté du carré est *impair* ou *pairement pair*, le problème admet non-seulement une solution, mais en général un grand nombre. Dans ce cas, l'analyse d'Euler conduit facilement aux solutions cherchées.

En définitive, ce mémoire très étendu contient un grand nombre d'observations très importantes pour la doctrine des combinaisons, ainsi que pour la théorie générale des carrés magiques.

REMARQUES SUR LA SECTION TROISIÈME.

A la subdivision *a*) se rapportent:

§ 13. Le mémoire III (N. 25 de l'Index) qui contient la résolution des équations indéterminées du premier degré à deux inconnues.

§ 14. Le commencement du mémoire XXI (N. 34) qui contient la résolution de l'équation indéterminée

$$x^3 + y^3 + z^3 = v^3.$$

§ 15. Le second problème du mémoire XXXI (N. 69) qui consiste dans la réduction de la formule

$$(t^2x^2 + u^2y^2)(u^2x^2 + t^2y^2)$$

à un carré.

§ 16. Le troisième paragraphe du mémoire XLV (N. 19) dans lequel on trouve la méthode pour réduire la formule $\left(\frac{x^2+1}{x}\right)^2 + \left(\frac{y^2+1}{y}\right)^2$ à un carré.

A la subdivision *b*):

§ 17. Le quatrième paragraphe du mémoire XLV (N. 19) qui contient la résolution des deux équations indéterminées simultanées $x + y = u^2$, $x^2 + y^2 = v^4$.

A la subdivision *c*):

§ 18. La fin du mémoire LXXIII (N. 81) qui contient la résolution des trois équations indéterminées simultanées: $ab - cd = u^2$, $ac - bd = v^2$, $bc - ad = w^2$.

§ 19. La fin du memoire LXXX (N. 65) qui contient la résolution des trois équations indéterminées simultanées:

$$a^2b^2+c^2d^2=u^2,\quad a^2c^2+b^2d^2=v^2,\quad a^2d^2+b^2c^2=w^2.$$

§ 20. Le premier problème du mémoire XC (N. 83) qui consiste à réduire à des carrés les trois formules:

$$vx+v+x,\quad vy+v+y,\quad xy+x+y.$$

A la subdivision *e*):

§ 21. La seconde question du mémoire XXXII (N. 80) et l'appendice dont il est suivi.

§ 22. Le second paragraphe du mémoire XLV (N. 19) qui contient la résolution des six équations indéterminées simultanées:

$$mn+1=l^2$$
$$m(m+n+2l)+1=(l+m)^2$$
$$n(m+n+2l)+1=(l+n)^2$$
$$4ml(l+m)(l+n)+1=(2l^2+2lm-1)^2$$
$$4nl(l+m)(l+n)+1=(2l^2+2ln-1)^2$$
$$4l(m+n+2l)(l+m)(l+n)+1=(4l^2+2lm+2ln-1)^2$$

auxquelles on est conduit en se proposant de *trouver quatre nombres tels, que le produit de deux quelconques de ces nombres, augmenté de l'unité, se réduise toujours à un carré.*

§ 23. Le sixième paragraphe du même mémoire XLV (N. 19) qui contient la solution du problème suivant: *trouver cinq nombres tels, que le produit de deux quelconques de ces nombres, augmenté de l'unité, se réduise toujours à un carré.* Cette question donnera lieu aux dix équations indéterminées simultanées:

$$xy+1=\square,\quad xz+1=\square,\quad xu+1=\square,\quad xv+1=\square,\quad yz+1=\square,$$
$$yu+1=\square,\quad yv+1=\square,\quad zu+1=\square,\quad zv+1=\square,\quad uv+1=\square,$$

le signe $\square$ désignant un carré complet.

Mélanges.

89. XXIV. *Solution d'une question curieuse qui ne paraît soumise à aucune analyse.* (*T.* I, *p.* 337.)

La question, traitée dans ce mémoire, consiste à *faire parcourir à un cavalier toutes les cases d'un échiquier, sans jamais repasser deux fois par la même, et en commençant par une case donnée.* L'analyse, employée par **Euler**, lui permet en outre de résoudre la question non seulement par rapport à l'échiquier ordinaire, composé de 64 cases, mais aussi pour des figures très variées, dont il donne des exemples à la fin de son mémoire. Ce travail, pour le fond, se rapporte à la géométrie de position, et, par l'analyse qui y est employée, à la théorie des nombres.

90. LI. *De summa seriei ex numeris primis formatae*

$$\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\frac{1}{13}-\frac{1}{17}+\frac{1}{19}+\frac{1}{23}-\frac{1}{29}+\frac{1}{31}-\textit{etc.}$$

ubi numeri primi formae $4n-1$ *habent signum*

Sur la sommation de la série réciproque des nombres premiers

$$\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\frac{1}{13}-\frac{1}{17}+\frac{1}{19}+\text{etc}$$

dans laquelle les termes positifs se rapportent aux dénominateurs de la forme $4n-1$, et les termes négatifs à

positivum, formae autem $4n+1$ *signum negativum.* (*T.* II, *p.* 116.)

ceux de la forme $4n+1$. La fin du mémoire contient des recherches sur la sommation des différentes séries que l'on obtient en élevant à des puissances impaires les termes successifs de la suite primitive

$$\frac{1}{3}-\frac{1}{5}+\frac{1}{7}+\frac{1}{11}-\text{etc.}$$

91. XLIX. *De relatione inter ternas pluresve quantitates instituenda.* (*T.* II, *p.* 99.)

La question traitée dans ce petit mémoire consiste à trouver les valeurs *minima* des trois nombres entiers α, β, γ satisfaisant, approximativement, à l'équation indéterminée $\alpha A = \pm \beta B \mp \gamma C$, les quantités A, B et C étant données, et pouvant être en général des nombres irrationnels ou même transcendants. Ce problème, comme on le voit, se rapportera à la résolution de l'équation indéterminée du premier degré à trois inconnues, quand on aura exprimé rationnellement, par approximation, les quantités données A, B et C.

92. XXVIII. *De inventione quotcunque mediarum proportionalium citra radicum extractionem.* (*T.* I, *p.* 401.)

Ce mémoire contient des recherches d'un haut intérêt sur la détermination approximative, en nombres rationnels, des moyennes proportionelles, sans qu'on ait besoin de recourir aux extractions de racines.

93. XCI. *Theorema arithmeticum ejusque demonstratio.* (*T* II, *pag.* 588, inédit.)

Ce mémoire, dont la fin manque, contient la démonstration d'une identité curieuse, dont voici l'énoncé:

Soient m *nombres inégaux quelconques* a, b, c, d, e, *etc. Si l'on forme les produits*

$$(a-b)(a-c)(a-d)(a-e)\ldots = A,$$
$$(b-a)(b-c)(b-d)(b-e)\ldots = B,$$
$$(c-a)(c-b)(c-d)(c-e)\ldots = C,$$
$$(d-a)(d-b)(d-c)(d-e)\ldots = D,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

on aura toujours identiquement

$$\frac{a^n}{A}+\frac{b^n}{B}+\frac{c^n}{C}+\frac{d^n}{D}+\ldots = 0,$$

n *étant un entier inférieur à* $m-1$.

Il est aussi question de ce théorème d'analyse dans la *Correspondance mathématique et physique de quelques célèbres géomètres du* XVIII *siècle* (Tome I, lettres CLXX et CLXXII, pages 659 et 665).

SCRIPTA ACADEMICA ET COLLECTIONES

in quibus singulae hujus libri dissertationes primum editae fuerunt, adjecto, pro quovis tomo, anno emissionis.

Paginae numeris arabicis indicatae referuntur ad primas editiones; numeri romani minores ad locum, quem singulae commentationes in nostra Collectione occupant. Hanc ob causam indicatio tomi supervacanea visa est: Commentationes nempe

I ad XLI continentur Tomo I,
XLII ad LXXXVIII » Tomo II.

Acad. Petropol.

Commentarii	T. VI.	1738. p. 103. I. p. 175. II.
	VII.	1740. p. 46. III.
	VIII.	1741. p. 141. IV.
	X.	1747. p. 125. V.
	XIV.	1751. p. 151. VI.
Nov. Comment.	T. I.	1750. p. 20. VII.
	II.	1751. p. 49. VIII.
	III.	1753 p. 125. IX.
	IV.	1758. p. 3. XII.
	V.	1760. p. 3. XV. p. 59. XI. p. 75. XVI.
	VI.	1761. p. 85. XVIII. p. 155. XIV. p. 185. XIII.
	VII.	1761. p. 49. XIX.
	VIII.	1763. p. 64. XVII. p. 74. XX. p. 105. XXI.
	IX.	1764. p. 3. XXII. p. 99. XXV.
	XI.	1767. p. 28. XXIII.
	XIII.	1769. p. 67. XXVI.
	XIV, 1.	1770. p. 168. XXVII. p. 188. XXVIII.
	XV.	1771. p. 29. XXIX. p. 75. XXX.
	XVII.	1773. p. 24. XXXII. p. 64. XXXIII.
	XVIII.	1774. p. 85. XXXVII. p. 171. XXXVI. p. 185. XXXIX. p. 218. XLI.
	XIX.	1775. p. 112. XLVI. p. 132. XLVII.
	XX.	1776. p. 48. XXXI.
Acta	T. I, 2.	1780. p. 48. XXXVIII. *
	II, 2.	1781. p. 85. LXXII.
	III, 1.	1782. p. 30. LXXXIV.
	IV, 1.	1783. p. 56. L.
	IV, 2.	1784. p. 18. LII. p. 38. LIII.
Nova Acta	T. I.	1787. p. 47. LV.
	IX.	1795. p. 3. LVI.
	X.	1797. p. 27. LVII. p. 63. LXII.
	XI.	1798. p. 78. LVIII.
	XII.	1801. p. 22. LXIII. p. 101. LXIX.
	XIII.	1802. p. 14. LIX. p. 45. LXVIII.
	XIV.	1805. p. 3. LX. p. 11. LVI.
	XV.	1806. p. 29. LXIV.
Mémoires	T. II.	1810. p. 10. LXXI.
	IV.	1813. p. 3. LXV.
	V.	1815. p. 3. LXVII. p. 73. LXXIII.
	VI.	1818. p. 54. LXXIV.
	VII.	1820. p. 3. LXXXVII. p. 10. LXXXVIII.
	VIII.	1822. p. 3. LXXVII.
	IX.	1824. p. 3. LXXV. p. 14. LXXVIII.
	X.	1826. p. 3. LXXVI.
	XI.	1830. p. 1. LXXIX. p. 12. LXXX. p. 31. LXXXI. p. 46. LXXXII. p. 49. LXXXIII. p. 58. LXXXV. p. 69. LXXXVI.
Opusc. anal.	T. I.	1783. p. 64. XXXIV. p. 121. XXXV. p. 211. XL. p. 268. XLII. p. 296. XLIII. p. 310. XLIV. p. 329. XLV.
	II.	1785. p. 3. XLVIII. p. 91. XLIX. p. 240. LI. p. 275. LIV

Acad. Berolin.

Mémoires	T. XV.	1766. p. 310. XXIV.
Nouv. Mém.		1772. p. 35. Addit. T. I.
		1776. p. 337. LXVI.
Opusc. var. arg.	T. II.	1750. p. 23. X.
Acta Erud. Lips.		1747. p. 267. Addit. T. II. 2.
		1773. p. 193. XXXVIII. *

Soc. Vlissing.

Verhandelingen	T. IX.	1782. p. 85. LXX.

SUPPLEMENTA PROOEMII.

1. Ad pag. XVII, N. 56 et pag. XVIII, N. 57.

Harum duarum commentationum apographa die 20mo demum Januarii (1mo Februarii) ad me pervenerunt, cum ipsum prooemium typis jam expressum esset. Quibus curiose perlectis, utramque in additamenta tomi secundi recipere censui, nulla earum adhibita contractione. Commentatio *de numeris amicabilibus* in analysi differt ab altera, quam exhibet operis nostri N. X, T. I pag. 102 ad 145. Inter talium numerorum exempla inveniuntur paria duo ex quatuor illis, quae recensus in Actis Lips. anni 1747 datus exhibet, sed quae desunt in catalogo numerorum amicabilium seriore eoque locupletiore, quem Opuscula var. arg. offerunt (Vide Prooem. p. XXVI N. 11). Tractatus finitur tabula, summas exhibente divisorum, quos habent numeri primi eorumque potestates; quae tabula ad unguem convenit cum ea, quam offert T. I pag. 104 ad 109, cum in utraque idem numerus primus 79 desit. Cujus tabulae repetundae nulla itaque ratio fuit.

Commentationi inscriptae: *Découverte d'une loi tout extraordinaire des nombres, par rapport à la somme de leurs diviseurs*, nil quidem inest, nisi quod melius et amplius in serioribus expositum sit tractatibus, quos tomus primus noster offert. Nihilo minus non caret hic libellus auctoritate aliqua in historia et inventorum Euleri et eruditionis progredientis recte cognoscenda. Quam ob rem lectoribus non ingratum fore speramus, quod brevem hanc commentationem, eamque in digerenda materia a cognatis diversam, contra priorem nostram opinionem, jamjam Additamentis adjecimus. (Vide etiam Prooem. pag. XXIV N. 1).

2. Additamenti pagg. XXIV ad XXVIII dati, quod opera Euleri hucusque non consignata indicat, continuatio.

Ad titulos 16 ibi datos jamjam 17^{mum} licet adjicere libelli, nobis a cel. collega Ostrogradskio indicati, qui omnium Euleri lucubrationum ultimam continet, ideoque ex opposito respondet primo illi specimini, cujus sub N. 6 pag. XXVI mentio est facta. Scilicet in Actis Parisiensibus anni 1781 pag. 265 ad 268 tractatulus invenitur ita inscriptus: *Calculs sur les ballons aérostatiques, faits par feu M.* Léonard Euler, *tels qu'on les a trouvés sur*

son ardoise, après sa mort arrivée le 7 *Septembre* 1783, quem filius Joannes Albertus descriptum Parisios miserat. Verba introitus honori sunt non minus magno Geometrae, quam inclytae Academiae, quae sodalem defunctum tali dignata sit memoria. In Euleri laudatione a N. Fussio edita calculorum de aërostatis perfectorum mentio quidem facta est (vide pag. XLVII), qui vero ipsam commentatiunculam, quae 1784 demum prodiit, in catalogo *A* non retulit, ne inter Inedita quidem, quae, ut notum est, solos complectebatur tractatus Academiae Petropolitanae traditos et in ejus tabulario depositos. Quidquid seu imperfectum, seu Academiae nondum oblatum superaerat, id tum temporis laudationis auctori, cum nondum familiae Eulerianae affinis exstiterit, prorsus ignotum fuisse ex silentio ejus apparet.

3. Ad finem Prooemii pag. XXVII, super lineam.

Quamquam recensus scriptorum Euleri his nostris studiis incrementum cepit satis luculentum, cum, Ineditis non respectis, 38 libri accesserint hucusque non consignati, tantum tamen abest ut confidamus, catalogum librorum editorum nunc penitus absolutum esse, cum concedendum sit, in Actis Societatum minorum, in libellis periodicis et collectionibus, nonnullas fortasse etiamnum latere Euleri commentationes. Quas ab oblivione vindicare in futurum quoque curae nobis erit. Jam supra exemplum attulimus tractatus illius Divionem missi, quem praemium obtinuisse et editum fuisse vix est quod dubitemus. Neque vero mirum erit, si aliqui tractatus inveniuntur, occasione oblata seorsim editi, quorum memoria temporis decursu interierit, similes opusculo, quod de Revelatione divina tuenda olim composuit (N. 745 catalogi *B*: *Rettung der Offenbarung gegen die Einwürfe der Freigeister*). Verum enimvero si auctores nonnulli volunt, opera majora Euleri complura, anonyme edita, e commercio librario ita penitus excidisse, ut in catalogis scriptorum ne mentio quidem fieret eorum: hoc judicio bibliographos in errorem induci nobis persuasum est, nisi res argumentis probetur validis.

Ita in brevi prooemio versioni gallicae Arithmetices Eulerianae praemisso, quam vol. III operum Euleri Bruxellis editorum [1] exhibet, cl. Duboisius nos docet, huic operi priora fuisse duo alia Euleri opera majora, alterum Institutiones disciplinae mercatoriae (*Guide du commerce*), duobus voluminibus 4to compositum, alterum de calculo syngrapharum tractatus (*Traité des changes et arbitrages*) unius vol. 4to. Haec opera, si fuerunt, Petropoli prodiisse opus est, ubi Eulerus inde ab aetatis anno vicesimo degerat, et anno 1738 *Arithmeticam* scripsit in usum Gymnasii academici [2]. Sed quomodo explicari poterit, talia

(1) Hanc editionem vix fas erit versionem nuncupare, cum librum exhibeat penitus retractatum.

(2) Hoc opus sicut fortasse et illud systema Physices, de quo supra pag. XIV. XV sermo est, Eulerus publica auctoritate composuit. Simili modo G. W. Krafftius Institutiones scripsit geographicas. Inter manuscripta Euleri initia reperiuntur cursus elementaris geometrici germanice conscripta. Origo Algebrae, multo serioris, nota est.

opera N. Fussium vitam Euleri Petropoli scribentem fugisse. Nisi Duboisius expressis verbis opera haec anonyme prodiisse dixisset, suspicarer nominis mutationem obtinere, cum memoria obscura mihi adsit, Eulerum aliquem citari inter auctores rei mercatoriae, cui nil nisi nomen cum magno nostro Geometra commune sit.

Alia res, quam idem ille editor Arithmetices Eulerianae indicat, majori digna videtur fide, quamquam nobis prorsus sit nova, Joannem Bernoullium minorem scilicet, qui primus Algebram Eulerianam Berolini gallice vertit, jam antea ejusdem auctoris Arithmeticam eodem sermone reddidisse. Hujus vero versionis exemplum videre nunquam nobis contigit, neque ipse Bernoullius in Algebrae translatae introductione ullam ipsius facit mentionem. Hoc saltem conjicere licet, versionem Bernoullii, si re vera exstat, majori gaudere fide, quam ipsius cl. Duboisii versionem recentiorem.

Denique in libro aliquo, qui inscriptus est: J. W. Müller's *Auserlesene mathematische Bibliothek.* Nürnberg 1820. 8°, pag. 5 citata invenimus Euleri (Leonh.) *Elementa mathematica*, 2 tomis Lausannae 1748. 4to edita, opus nobis prorsus ignotum. At nulli dubitare possumus, quin hoc citatum originem traxerit ex male mutato titulo operis notissimi *Introductionis in Analysin infinitorum*, quae eodem anno 1748, ibidem Lausannae, prodiit duobus voluminibus 4to; quamquam mirandum est, librum hunc suo titulo in ejusdem Mülleri opere citari, tribus allatis editionibus latinis et una gallica.

Si qui viri docti de his aliisque dubiis certiora nos potuerint docere, grato animo emendationes accipiemus.

M. Februario 1849.

P. H. F.

CONSPECTUS TOMI PRIORIS.

Index Commentationum

in hoc tomo priori contentarum,

ordine, quantum fieri potuit, chronologico dispositus.

CORRIGENDA ET EMENDANDA IN TOMO I.

Pag. 55. l. 3. ab i. loco $a^{2^n}q + b^{2^n}q$ lege $a^{2^n q} + b^{2^n q}$.

In inscriptione paginarum 58. 76. 92. 100. 126. 144. 158. 176 loco E. Euleri lege L. Euleri.

Pag. 73. l. 4. a s. loco Haude lege Naudé.

Pag. 80. l. 11. a s. loco 6 lege n.

Pag. 86. l. 1 ab i. loco manifestum lege manifesta.

Pag. 91. l. 15 a s. loco haberi lege habere.

Pag. 105. in tabula pro summis divisorum deest numerus primus 79 cum potentiis. Haec omissio ita supplenda est:

Num.	Summa divisorum
79	$2^4.5$
79^2	$3.7^2.43$
79^3	$2^5.5.3121$.

Pag. 552. l. 7 a s. in denominatore loco ζ^λ lege $\zeta\lambda$.

LEONHARDI EULERI

COMMENTATIONES ARITHMETICAE

EX ANNIS 1732 AD 1772.

I.

Observationes de theoremate quodam Fermatiano, aliisque ad numeros primos spectantibus.

(Comment. VI. 1732 — 33. p. 103.)

Notum est hanc quantitatem $a^n + 1$ semper habere divisores, quoties n sit numerus impar, vel per imparem praeter unitatem divisibilis. Namque $a^{2m+1} + 1$ dividi potest per $a + 1$, et $a^{p(2m+1)} + 1$ per $a^p + 1$, quicunque etiam numerus loco a substituatur. Contra vero, si n fuerit ejusmodi numerus, qui per nullum numerum imparem nisi unitatem dividi possit, id quod evenit, quando n est dignitas binarii, nullus numeri $a^n + 1$ potest assignari divisor. Quamobrem si qui sunt numeri primi hujus formae $a^n + 1$, ii omnes comprehendantur necesse est in hac forma $a^{2^m} + 1$. Neque tamen ex hoc potest concludi $a^{2^m} + 1$ semper exhibere numerum primum quicquid sit a; primo enim perspicuum est, si a sit numerus impar, istam formam divisorem habituram 2. Deinde quoque, etiamsi a denotet numerum parem, innumeri tamen dantur casus, quibus numerus compositus prodit. Ita haec saltem formula $a^2 + 1$ potest dividi per 5, quoties est $a = 5b \pm 3$, et $30^2 + 1$ potest dividi per 17, et $50^2 + 1$ per 41. Simili modo $10^4 + 1$ habet divisorem 73; $6^8 + 1$ habet divisorem 17, et $6^{128} + 1$ est divisibilis per 257. At hujus formae $2^{2^m} + 1$, quantum constat ex tabulis numerorum primorum, quae quidem non ultra 100000 extenduntur, nullus detegitur casus, quo divisor aliquis locum habeat. Hac forte aliisque rationibus Fermatius adductus enunciare non dubitavit $2^{2^m} + 1$ semper esse numerum primum, hocque ut eximium theorema Wallisio aliisque Mathematicis Anglis demonstrandum proposuit. Ipse quidem fatetur se ejus demonstrationem non habere, nihilo tamen minus asserit esse verissimum. Utilitatem ejus autem hanc potissimum praedicat, quod ejus ope facile sit numerum primum quovis dato majorem exhibere, id quod sine hujusmodi universali theoremate foret difficillimum. Leguntur haec in Wallisii *Commercio Epistolico* tomo ejus Operum secundo inserto, epistola penultima. Exstant etiam in ipsius Fermatii Operibus p. 115 sequentia. „Cum autem numeros a binario quadratice in se ductos et unitate auctos esse semper numeros primos apud me constet, et jam dudum Analystis illius theorematis veritas fuerit significata, nempe esse primos 3, 5, 17, 257, 65537, etc. in infinit. nullo negotio etc.“

Veritas istius theorematis elucet, ut jam dixi, si pro m ponatur 1, 2, 3 et 4; prodeunt enim hi numeri 5, 17, 257, et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed nescio, quo fato eveniat, ut statim sequens nempe $2^{2^5}+1$ cesset esse numerus primus, observavi enim his diebus, longe alia agens, posse hunc numerum dividi per 641, ut cuique tentanti statim patebit. Est enim $2^{2^5}+1 = 2^{32}+1 = 4294967297$. Ex quo intelligi potest, theorema hoc etiam in aliis, qui sequuntur, casibus fallere, et hanc ob rem problema de inveniendo numero primo quovis dato majore etiam nunc non esse solutum.

Considerabo nunc etiam formulam 2^n-1, quae quoties n non est numerus primus, habet divisores, neque tantum 2^n-1 sed etiam a^n-1. Sed si n sit numerus primus, videri posset etiam 2^n-1 semper talem exhibere: hoc tamen asseverare nemo est ausus quantum scio, cum tam facile potuisset refelli. Namque $2^{11}-1$ i. e. 2047 divisores habet 23 et 89, et $2^{23}-1$ dividi potest per 47. Video autem Cel. Wolfium non solum hoc in *Elem. Matheseos* editione altera non advertisse, ubi numeros perfectos investigat, atque 2047 inter primos numerat; sed etiam 511 seu 2^9-1 pro tali habet, cum tamen sit divisibilis per 2^3-1 i. e. 7. Dat autem $2^{n-1}(2^n-1)$ numerum perfectum, quoties 2^n-1 est primus, debet ergo etiam n esse numerus primus. Operae igitur pretium fore existimavi eos notare casus, quibus 2^n-1 non est numerus primus, quamvis n sit talis. Inveni autem hoc semper fieri, si sit $n = 4m-1$, atque $8m-1$ fuerit numerus primus, tum enim 2^n-1 semper poterit dividi per $8m-1$. Hinc excludendi sunt casus sequentes: 11, 23, 83, 131, 179, 191, 239, etc. qui numeri pro n substituti reddunt 2^n-1 numerum compositum. Neque tamen reliqui numeri primi omnes loco n positi satisfaciunt, sed plures insuper excipiuntur, sic observavi $2^{37}-1$ dividi posse per 223, $2^{43}-1$ per 431, $2^{29}-1$ per 1103, $2^{73}-1$ per 439, omnes tamen excludere non est in potestate. Attamen asserere audeo praeter hos casus notatos, omnes numeros primos minores quam 50, et forte quam 100, efficere $2^{n-1}(2^n-1)$ esse numerum perfectum, sequentibus numeris pro n positis: 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, unde 11 proveniunt numeri perfecti. Deduxi has observationes ex theoremate quodam non ineleganti, cujus quidem demonstrationem quoque non habeo, verum tamen de ejus veritate sum certissimus. Theorema hoc est: a^n-b^n semper potest dividi per $n+1$, si $n+1$ fuerit numerus primus, atque a et b non possint per eum dividi; eo autem difficiliorem puto ejus demonstrationem esse, quia non est verum nisi $n+1$ sit numerus primus. Ex hoc statim sequitur 2^n-1 semper dividi posse per $n+1$, si fuerit $n+1$ numerus primus, seu cum omnis primus sit impar praeter 2, hicque ob conditiones theorematis, quia est $a=2$, non possit adhiberi, poterit $2^{2m}-1$ semper dividi per $2m+1$, si $2m+1$ sit numerus primus. Quare etiam vel 2^m+1 vel 2^m-1 dividi poterit per $2m+1$. Deprehendi autem 2^m+1 posse dividi, si fuerit $m = 4p+1$, vel $4p+2$, at 2^m-1 habebit divisorem $2m+1$, si $m = 4p$, vel $4p-1$. Haec persecutus in multa alia incidi theoremata non minus elegantia, quae eo magis aestimanda esse puto, quod vel demonstrari prorsus nequeant, vel ex ejusmodi propositionibus sequantur, quae demonstrari non possunt; primaria igitur hic adjungere visum est.

Theorema I. Si fuerit n numerus primus, omnis potentia exponentis $n-1$ per n divisa vel nihil vel 1 relinquit.

Theorema II. Manente n numero primo, omnis potentia, cujus exponens est $n^{m-1}(n-1)$, divisa per n^m vel 0 vel 1 relinquit.

Theorema III. Sint m, n, p, q, etc. numeri primi inaequales, sitque A minimus communis dividuus eorum unitate minutorum, puta ipsorum $m-1$, $n-1$, $p-1$, $q-1$, etc.; his positis dico omnem potentiam exponentis A, ut a^A, divisam per $mnpq$ etc. vel 0 vel 1 relinquere, nisi a dividi possit per aliquem horum numerorum, m, n, p, q, etc.

Theorema IV. Denotante $2n+1$ numerum primum, poterit 3^n+1 dividi per $2n+1$, si sit vel $n=6p+2$, vel $n=6p+3$: at 3^n-1 dividi poterit per $2n+1$, si sit vel $n=6p$, vel $n=6p-1$.

Theorema V. 3^n+2^n potest dividi per $2n+1$, si sit $n=$ vel $12p+3$, vel $12p+5$, vel $12p+6$, vel $12p+8$. Atque 3^n-2^n potest dividi per $2n+1$, si sit $n=$ vel $12p$, vel $12p+2$, vel $12p+9$, vel $12p+11$.

Theorema VI. Sub iisdem conditionibus, quibus 3^n+2^n, poterit etiam 6^n+1 dividi per $2n+1$; atque 6^n-1 sub iisdem, quibus 3^n-2^n.



II.

De solutione problematum Diophanteorum per numeros integros.

(Comment. VI. 1732 — 33. p. 175.)

§ 1. Quoties in problematibus Diophanteis solvendis pervenitur ad formulam, in qua plus una indeterminata non inest, maxime requiruntur numeri integri, qui loco indeterminatae positi quaesito satisfaciant. Hoc vero quando fieri non potest, numeris fractis acquiescere oportet. Observatum autem est, si in illa formula indeterminatae maxima dimensio fuerit quadratum, et ipsa formula debeat esse numerus quadratus, plerumque infinitos numeros integros problema solvere, qui inter se certa lege cohaereant, et seriem quandam constituant. Sed si formula vel debeat esse cubus aliave altior potentia, vel si indeterminata plures duabus habeat dimensiones, plus effici non potest, quam ut saltem numeri fracti eruantur.

§ 2. Ita autem hujusmodi problematum omnium ratio est comparata, ut unum numerum satisfacientem divinatione inveniri oporteat, ex quo deinceps infiniti alii reperiri queant. Neque enim ad primum detegendum regula potest tradi, cum casus possint occurrere, qui omnino nullam solutionem admittunt, cujusmodi est $3x^2 + 2$, quae formula nunquam fieri potest quadratum. Quamobrem in sequentibus semper ponemus, unicum tantum casum esse cognitum, quo conditioni problematis satisfiat, atque regulam dabimus, qua ex illo innumerabiles alii elici possint.

§ 3. Proposita igitur sit haec formula $ax^2 + bx + c$, quae debeat esse numerus quadratus. Sintque a, b et c numeri integri, et requirantur quoque numeri integri loco x substituendi. Datus autem sit numerus n, qui loco x positus reddat formulam $ax^2 + bx + c$ quadratum. Erit ergo $an^2 + bn + c$ numerus quadratus, cujus radix sit m. Jam ad alium numerum satisfacientem ex hoc dato n inveniendum, pono eum esse $\alpha n + \beta + \gamma \sqrt{(an^2 + bn + c)}$, huncque valorem loco x substitutum reddere $ax^2 + bx + c$ quadratum, cujus radix sit $\delta n + \varepsilon + \zeta \sqrt{(an^2 + bn + c)}$. Perspicuum enim est illum numerum loco x substituendum fore rationalem ob $an^2 + bn + c$ quadratum, numeros autem integros hoc modo reperiri, si modo sit n numerus integer, mox apparebit.

§ 4. Substituatur igitur $\alpha n + \beta + \gamma \sqrt{(an^2 + bn + c)}$ loco x in $ax^2 + bx + c$, hocque facto prodibit

$$\begin{aligned} &(a\alpha^2 + a^2\gamma^2)\, n^2 \\ &+ (2a\alpha\beta + ab\gamma^2 + b\alpha)\, n \\ &+ a\beta^2 + ac\gamma^2 + b\beta + c \\ &+ (2a\alpha\gamma n + 2a\beta\gamma + b\gamma) \sqrt{(an^2 + bn + c)}. \end{aligned}$$

Sed quia hujus radicem quadratam ponimus $\delta n + \varepsilon + \zeta \sqrt{(an^2 + bn + c)}$, erit hinc etiam $ax^2 + bx + c$ aequalis sequenti quantitati:

$$\begin{aligned} &(\delta^2 + a\zeta^2)\, n^2 + (2\delta\varepsilon + b\zeta^2)\, n + \varepsilon^2 + c\zeta^2 \\ &+ (2\delta\zeta n + 2\varepsilon\zeta) \sqrt{(an^2 + bn + c)}. \end{aligned}$$

His duabus formis inter se aequatis, habebuntur sequentes aequationes:

$$a\alpha^2 + a^2\gamma^2 = \delta^2 + a\zeta^2,\ 2a\alpha\beta + ab\gamma^2 + b\alpha = 2\delta\varepsilon + b\zeta^2,\ a\beta^2 + ac\gamma^2 + b\beta + c = \varepsilon^2 + c\zeta^2,$$
$$2a\alpha\gamma = 2\delta\zeta,\ 2a\beta\gamma + b\gamma = 2\varepsilon\zeta.$$

Ex quibus elicitur $\delta = \frac{a\alpha\gamma}{\zeta}$ et $\varepsilon = \frac{2a\beta\gamma + b\gamma}{2\zeta}$, et valor ipsius δ in prima aequatione substitutus dat: $\alpha^2\zeta^2 + a\gamma^2\zeta^2 = a\alpha^2\gamma^2 + \zeta^4$, quae in duas resolvitur $\zeta^2 = \alpha^2$, et $\zeta^2 = a\gamma^2$. Harum autem posterior, nisi sit a quadratum, locum habere nequit. Habebimus ergo $\zeta = \alpha$, et secunda aequatio, factis substitutionibus hisce, similiter in has resolvetur $a\gamma^2 = \alpha^2$, et $\beta = \frac{b(\alpha - 1)}{2a}$, quarum iterum posterior tantum locum habet. His inventis, tertia tandem aequatio dabit $\alpha = \sqrt{(a\gamma^2 + 1)}$: inveniri igitur debet valor pro γ, quo $a\gamma^2 + 1$ fiat quadratum.

§ 5. Sit p iste numerus, qui loco γ substitutus reddat $a\gamma^2 + 1$ quadratum, et hujus radix ponatur q; ita ut sit $q = \sqrt{(ap^2 + 1)}$, erit $\alpha = q$, $\gamma = p$, $\beta = \frac{b(q-1)}{2a}$, $\delta = ap$, $\varepsilon = \frac{bp}{2}$ et $\zeta = q$. Ex his colligitur sequens theorema:

> Si $ax^2 + bx + c$ est quadratum casu quo $x = n$, erit quoque quadratum casu, quo $x = qn + \frac{bq - b}{2a} + p\sqrt{(an^2 + bn + c)}$; ejusque quadrati radix erit $apn + \frac{bp}{2} + q\sqrt{(an^2 + bn + c)}$.

Si ergo modo bp per 2 dividi potest, radix quadrati erit numerus integer, et propterea quoque valor ipsius x erit integer, seu $bq - b$ dividi poterit per $2a$.

§ 6. Quemadmodum autem ex n valore ipsius x dato inventus est alius $qn + \frac{bq - b}{2a} + pm$, posito m loco $\sqrt{(an^2 + bn + c)}$; ita hac quantitate tanquam n tractata, quo casu loco m sumi debebit $apn + \frac{bp}{2} + qm$, eruetur denuo alius valor, qui loco x substitutus quaesito satisfacit, scilicet hic:

$$2ap^2n + bp^2 + 2pqm + n,$$ quadrati vero hinc orti radix erit $$2apq + bpq + 2ap^2m + m.$$

Consideretur jam illa quantitas ut n et haec ut m, habebitur quartus valor ipsius x satisfaciens hic:

$$4ap^2qn + 2bp^2q + 4ap^3m + qn + \frac{b(q-1)}{2a} + 3pm.$$

Et radix quadrati respondentis erit:

$$4a^2p^3n + 2bp^3 + 4ap^2qm + 3apn + \frac{3bp}{2} + qm.$$

§ 7. Valores ipsius x satisfacientes, una cum radicibus quadratorum respondentium ergo ita se habebunt, ut sequitur:

	Valores ipsius x	Valores $\sqrt{(ax^2 + bx + c)}$
I.	n	m
II.	$qn + pm + \frac{b(q-1)}{2a}$	$apn + qm + \frac{bp}{2}$
III.	$2q^2n + 2pqm + \frac{b(q^2-1)}{a}$ $-n$	$2apqn + 2q^2m + bpq$ $-m$
IV.	$4q^3n + 4pq^2m + \frac{b(4q^2-3q-1)}{2a}$ $-3qn - pm$	$4apq^2n + 4q^3m + 2bpq^2$ $-apn - 3qm - \frac{bp}{2}$
V.	$8q^4n + 8pq^3m + \frac{4bq^2(q^2-1)}{a}$ $-8q^2n - 4pqm$ $+n$ etc.	$8apq^3n + 8q^4m + 4bpq^3$ $-4apqn - 8q^2m - 2bpq$ $+m$ etc.
	Hujus progressionis haec est lex:	Hujus progressionis haec est lex:
	term. quicunque A	E
	hunc sequens B	F
	$2qB - A + \frac{b(q-1)}{a}$	$2qF - E$.

Hae igitur progressiones, quousque libuerit, exiguo labore continuantur.

§ 8. Perspicitur ex his formis alternos ad minimum terminos efficere $ax^2 + bx + c$ numerum quadratum integrum; atque omnia omnino quadrata fieri numeros integros, si fuerit bp numerus par. Omnes autem ipsius x valores erunt numeri integri, si $b(q-1)$ dividi poterit per $2a$; sin vero hoc non fuerit, saltem alterni ipsius x valores erunt numeri integri, nam $qq - 1$ i. e. ap^2 semper dividi poterit per a, si quidem, ut ponimus, p et q sint numeri integri. Praeterea notandum est in terminis istis etiam m negative accipi posse, qua ratione numerus solutionum quandoque duplicatur.

§ 9. Intelligitur etiam, si a sit numerus quadratus, solutionem in numeris integris exhiberi non posse, nisi forte $ax^2 + bx + c$ vel ipsum est quadratum, vel numero quadrato fieri potest aequale. Hanc ob rem exclusimus supra eos casus, quibus a erat quadratum, quia hic tantum de numeris integris problema solventibus praecepta tradere instituimus. Nam si a est quadratum; nullus numerus integer potest exhiberi, qui loco p positus efficiat $ap^2 + 1$ quadratum, praeter 0. Hoc vero casu omnes valores ipsius x manent n, nullusque ergo alius, nisi is, qui divinatione est inventus, eruitur.

§ 10. Quoties autem a non est numerus quadratus, semper numerus integer potest assignari, qui loco p positus efficiat $ap^2 + 1$ quadratum. Quamobrem his casibus, si unicum casum elicuerimus, quo $ax^2 + bx + c$ fit quadratum, simul quoque casus infinitos exhibere poterimus, qui $ax^2 + bx + c$ in quadratum transmutent. Proposita igitur formula $ax^2 + bx + c$ hoc erit agendum: primo conjectura detegi debebit valor ipsius x in integris, qui reddat $ax^2 + bx + c$ quadratum. Deinde etiam quaeri debet valor ipsius p, quo $ap^2 + 1$ etiam fiat quadratum. Hisque inventis ope progressionum inventarum casus infiniti innotescent.

§ 11. Si c est quadratum, nempe $= dd$, statim apparet casus, quo $ax^2 + bx + d^2$ est quadratum, is enim est si $x = 0$. Ponamus ergo $n = 0$, eritque $m = d$, et valores ipsius x satisfacientes constituent hanc seriem: 0, $dp + \frac{b(q-1)}{2a}$, $2dpq + \frac{b(q^2-1)}{a}$, ... A, B, $2qB - A + \frac{b(q-1)}{a}$.

Quadratorum autem, quae hinc generantur, radices erunt: d, $dq+\frac{bq}{2}$, $d(2q^2-1)+bpq$, ... E, F, $2qF-E$. Harum serierum lex, ut et priorum (§ 7) perspicua est; sunt enim omnes recurrentes, seu quivis terminus ex duabus praecedentibus est compositus.

§ 12. Si $b=0$ et $d=1$, ut habeatur haec forma ax^2+1, ad quam, ut ex praecedentibus apparet, generalis ax^2+bx+c maximam partem reducitur. Hujus ergo valores ipsius x respondentes in hac serie progrediuntur: 0, p, $2pq$, $4pq^2-p$,..... A, B, $2qB-A$. Radices vero quadratorum productorum erunt sequentes: 1, q, $2q^2-1$, $4q^3-3q$,..... E, F, $2qF-E$. Si ergo unicus casus p, quo ap^2+1 fit quadratum constat, hujusmodi numeri infiniti habebuntur, qui in tractatione generalis formulae ax^2+bx+c loco p et q collocari possunt.

§ 13. Quo autem haec methodus ad quosvis casus possit accommodari, videamus primo, quos numeros, pro quolibet ipsius a valore, literis p et q tribui oporteat. Debet autem p talis esse numerus, qui ap^2+1 reddat quadratum, hujusque radix erit q. Perspicuum quidem est, si unicus pro p habeatur valor idoneus, simul quoque infinitos haberi; attamen hic unicum duntaxat eumque minimum praeter 0 adhiberi convenit. Nam reliqui sequentes, qui sunt $2pq$, $4pq^2-p$, etc. solutionum numerum non multiplicant, cum valores tantum sequentes ipsius x in § 7 praebeant. Minimus autem ipsius p valor dabit omnes numeros ipsius x satisfacientes, quod majores non faciunt.

§ 14. Intelligatur igitur, quod si fuerit $a=e^2-1$, minimum ipsius p valorem fore 1, ipsiusque q, e. Deinde si fuerit $a=e^2+1$, tum esse $p=2e$, et $q=2e^2+1$. Atque si sit $a=e^2\pm 2$, erit $p=e$, et $q=e^2\pm 1$. Hujusmodi casus infiniti alii possunt definiri, quorum ingens numerus hoc continetur theoremate: si sit $a=\alpha^2e^{2b}\pm 2\alpha e^{b-1}$, erit $p=e$, et $q=\alpha e^{b+1}\pm 1$, ubi pro α etiam numeri fracti accipi possunt, dummodo illi per e^{b-1} multiplicati in integros transmutentur. Simili modo etiam si sit $a=(\alpha e^b+\beta e^\mu)^2+2\alpha e^{b-1}+2\beta e^{\mu-1}$, erit $p=e$, et $q=\alpha e^{b+1}+\beta e^{\mu+1}+1$. Atque etiam si sit $a=\frac{1}{4}\alpha^2k^2e^{2b}\pm\alpha e^{b-1}$, erit $p=ke$, et $q=\frac{1}{2}\alpha k^2e^{b+1}\pm 1$.

§ 15. Quoties igitur a est numerus, qui in istis formulis contineatur, statim apparet valor ipsius p et q. At si a hujusmodi fuerit numerus, qui nullo modo ad illas formulas potest reduci, peculiaris ad invenienda p et q adhibenda est methodus, qua olim jam usi sunt Pellius et Fermatius. Haecque methodus est universalis, et aeque succedit, quemcunque numerum denotet a. Praeterea etiam ideo hic potissimum est commendanda, quod minimum ipsius p valorem, qui hoc loco requiritur, exhibeat.

§ 16. Methodus haec exstat descripta in Operibus Wallisii, et hanc ob rem eam hic fusius non expono. Operandi tamen modum in unico exemplo ostendisse juvabit, cujus inspectio ad quaeque alia solvenda perducet. Oporteat nimirum determinari minimum ipsius p valorem, quo $31p^2+1$ fit quadratum. Ad hoc efficiendum sequens instituitur calculus:

$$\sqrt{(31p^2+1)}=q. \text{ Ergo } q>5p, \text{ ponatur itaque } q=5p+a$$

$$6p^2+1=10ap+a^2,\quad p=\frac{5a+\sqrt{(31a^2-6)}}{6},\quad p=a+b,$$

$$5a^2=2ab+6b^2+1,\quad a=\frac{b+\sqrt{(31b^2+5)}}{5},\quad a=b+c,$$

$$3b^2=8bc+5c^2-1,\quad b=\frac{4c+\sqrt{(31c^2-3)}}{3},\quad b=3c+d,$$

$$2c^2 = 10cd + 3d^2 + 1,\quad c = \frac{5d+\sqrt{(31d^2+2)}}{2},\quad c = 5d + e,$$

$$3d^2 = 10de + 2e^2 - 1,\quad d = \frac{5e+\sqrt{(31e^2-3)}}{3},\quad d = 3e + f,$$

$$5e^2 = 8ef + 3f^2 + 1,\quad e = \frac{4f+\sqrt{(31f^2+5)}}{5},\quad e = 2f - g,$$

$$f^2 = 12fg - 5g^2 + 1,\quad f = 6g + \sqrt{(31g^2+1)}.$$

Tamdiu scilicet hae operationes continuantur, quoad in media columna perveniatur ad $\sqrt{(31g^2+1)}$ ejusdem formae, quam habuit proposita $\sqrt{(31p^2+1)}$. Perspicuum jam est si ponatur $g=0$, fore $f=1$. Hincque retrogrediendo habebitur: $e=2$, $d=7$, $c=37$, $b=118$, $a=155$, $p=273$, atque $q=1520$.

§ 17. Quo autem non tanto opus sit labore ad valores ipsarum p et q inveniendos pro dato numero a, sequentem tabulam annexere visum est, in qua pro singulis valoribus ipsius a exhibentur minimi numeri, qui loco p substituti reddant ap^2+1 quadratum.

a	p	q	a	p	q	a	p	q
2	2	3	26	10	51	47	7	48
3	1	2	27	5	26	48	1	7
5	4	9	28	24	127	50	14	99
6	2	5	29	1820	9801	51	7	50
7	3	8	30	2	11	52	90	649
8	1	3	31	273	1520	53	9100	66249
10	6	19	32	3	17	54	66	485
11	3	10	33	4	23	55	12	89
12	2	7	34	6	35	56	2	15
13	180	649	35	1	6	57	20	151
14	4	15	37	12	73	58	2574	19603
15	1	4	38	6	37	59	69	530
17	8	33	39	4	25	60	4	31
18	4	17	40	3	19	61	226153980	1766319049
19	39	170	41	320	2049	62	8	63
20	2	9	42	2	13	63	1	8
21	12	55	43	531	3482	65	16	129
22	42	197	44	30	199	66	8	65
23	5	24	45	24	161	67	5967	48842
24	1	5	46	3588	24335	68	4	33

§ 18. Hic statim occurrit modus perfacilis extrahendi quam proxime radicem quadratam ex numero quocunque non quadrato a. Quia enim est $ap^2+1=q^2$ erit $\sqrt{a} = \frac{\sqrt{(q^2-1)}}{p}$, et, si q sit numerus valde magnus, erit $\sqrt{a} = \frac{q}{p}$ quam proxime. Sed loco p possunt poni singuli termini seriei

$0,\ p,\ 2pq,\ 4pq^2-p, \ldots\ldots A,\ B,\ 2qB-A$, et loco q singuli termini respondentes seriei hujus $1,\ q,\ 2q^2-1,\ 4q^3-3q, \ldots\ldots E,\ F,\ 2qF-E$ (§ 12). Sit hujus seriei terminus indicis $i=Q$, et illius terminus, cujus index etiam i est $=P$, erit $\sqrt{a}=\frac{Q}{P}$. Quia vero, quo magis continuantur hae series, majores quoque fiunt termini Q; eo propior reperietur $\sqrt{a}$ sumendis terminis serierum a primo longius distantibus. Sit exempli gratia $a=6$, erit $p=2$ et $q=5$, seriesque sibi invicem subscribantur ut sequitur, posteriore loco superiore posita:

1, 5, 49, 485, 4801, 47525, 470449, 4656965, etc.
0, 2, 20, 198, 1960, 19402, 192060, 1901198, etc.

Sumtis igitur ultimis terminis, erit $\frac{4656965}{1901198}$ ita propinquum radici quadratae ex 6, ut plus eam non excedat, quam hac fractione $\frac{1}{2(1901198)^2\sqrt{6}}$. Simili modo patet radicem quadratam ex 61 fore proxime aequalem $\frac{1766319049}{226153980}$. Quae quidem radix vera aliquantulum major est, sed excessus est minor quam $\frac{1}{2(226153980)^2\sqrt{61}}$.

§ 19. Quaerantur omnes numeri triangulares, qui sint simul quadrati; debebit $\frac{x^2+x}{2}$ esse quadratum. Quadratum igitur quoque erit $2x^2+2x$, ex quo fit, collatione cum formula ax^2+bx+d^2 (§ 11) instituta $a=2$, $b=2$, $d=0$. Sed quia est $a=2$, erit ex tabula superiore $p=2$ et $q=3$. Unde loco x substitui debebunt sequentes valores 0, 1, 8, 49, 288, 1681, 9800, etc. quo $\frac{x^2+x}{2}$ fiat quadratum. Quadratorum autem hinc ortorum radices tenebunt hanc seriem, 0, 1, 6, 35, 204, 1189, 6930, etc. Vel quadrata, quorum radices continentur in hac serie, erunt numeri triangulares. Seriei quidem hujus posterioris termini fiunt duplo majores, si formentur ex serie generali d, $dq+\frac{bp}{2}$, $d(2q^2-1)+bpq$ etc.; sed quia hi termini sunt radices ex $2x^2+2x$, debebunt dividi per 2, quo habeantur radices ex $\frac{x^2+x}{2}$.

§ 20. Numeri polygonales l laterum exprimuntur hac formula generali $\frac{(l-2)x^2-(l-4)x}{2}$, in qua x denotat radicem numeri polygonalis. Quo ergo hujusmodi numerus polygonalis sit quadratum, oportet $2(l-2)x^2-2(l-4)x$ esse quadratum. Statim autem unus casus apparet, quo quaesito satisfit, scilicet si $x=0$; fit enim ipsa formula $=0$. Quam ob rem habebimus $n=0$ et $m=0$, et formula cum generali ax^2+bx+c comparata prodit $a=2(l-2)$ et $b=-2(l-4)$, atque $c=0$. Fiat igitur $2(l-2)p^2+1=q^2$, eruut ipsius x valores, quibus $2(l-2)x^2-2(l-4)x$ seu hujus pars quarta $\frac{(l-2)x^2-(l-4)x}{2}$ i. e. ipse numerus polygonalis fit quadratum, sequentes: $0,\ \frac{-(l-4)}{2(l-2)}(q-1),\ \frac{-(l-4)}{l-2}(q^2-1), \ldots\ldots A,\ B,\ 2qB-A-\frac{(l-4)}{l-2}(q-1)$. Qui quidem numeri omnes, si $l>4$, sunt negativi, attamen affirmativi habebuntur valores ipsius x sumto q negativo, tum enim alterni termini erunt affirmativi. Deinde etiam si inventus sit numerus negativus pro x, qui sit $-k$, poterit numerus affirmativus dari, qui eundem numerum polygonalem producat, erit nempe $x=k+\frac{l-4}{l-2}$, sed nisi sit $\frac{l-4}{l-2}$ numerus integer, hi numeri affirmativi fiunt fracti, quos hic excludimus. Hanc ob rem alternis terminis superioris seriei, posito $-q$ loco q, contenti esse debemus. Radices vero quadratorum $2(l-2)x^2-2(l-4)x$ his casibus resultantium tenebunt hanc progressionem: $0,\ (l-4)p,\ 2(l-4)pq, \ldots\ldots E,\ F,\ 2qF-E$.

§ 21. Quo autem non alii numeri, nisi affirmativi et integri reperiantur, alium casum, quo $2(l-2)x^2-2(l-4)x$ fit quadratum, erui oportet, qui erit, si $x=1$; prodibit enim 4. Hanc ob rem ponatur $n=1$ et $m=2$, quo facto habebuntur pro x valores sequentes:

$$1,\ q+2p-\frac{(l-4)}{2(l-2)}(q-1),\ 2q^2-1+4pq-\frac{(l-4)}{l-2}(q^2-1),\ldots.A,\ B,\ 2qB-A-\frac{(l-4)}{l-2}(q-1).$$

Radices autem quadratae ex $\frac{(l-2)x^2-(l-4)x}{2}$ progredientur in hac serie:

$$1,\ \frac{lp}{2}+q,\ lpq+2q^2-1,\ldots\ldots E,\ F,\ 2qF-E.$$

Quo autem omnes ipsius x valores sint numeri integri, non quidem loco q minimum valorem, sed eum, qui reddat $\frac{l-4}{2(l-2)}(q-1)$ numerum integrum seligi convenit, id quod semper fieri poterit. Ut si quaerantur numeri pentagonales quadrati, erit $l=5$ et $a=6$, atque q erit numerus ex hac serie 1, 5, 49, etc. et ipsius p valores respondentes erunt 0, 2, 20, etc. Quo igitur $\frac{(l-4)}{2(l-2)}(q-1)$ $=\frac{1}{6}(q-1)$ sit numerus integer, sumi debet $q=49$, et $p=20$. Radices ergo numerorum pentagonalium, qui sunt quadrati, erunt: 1, 81, 7921, ... A, B, $98B-A-16$, qui numeri etiam in superiore serie (§ 20) continentur, si accipiatur $q=-5$; erunt enim termini alterni affirmativi. Horum autem numerorum pentagonalium radices quadratae erunt 1, 99, 9701, ... E, F, $98F-E$.

§ 22. Quia est $2(l-2)p^2+1=q^2$, manifestum est ex praecedentibus, si fuerit $2l-4$ quadratum, nullum numerum integrum loco p substitui posse. Hanc ob rem vel omnes numeri polygonales erunt quadrati, vel tantum nonnulli. Prius evenit, si $l=4$; nam omnes numeri tetragonales sunt simul quadrati. Posterius vero si sit $2l-4=16$ seu 36, seu 64 etc. his enim casibus alii non erunt quadrati, nisi 0 et 1. Si $2l-4=16$, erit $l=10$, ideoque numeri polygonales erunt decagonales, quorum forma est $4x^2-3x$. Nullusque numerus decagonalis est quadratus praeter 0 et 1 in integris.



III.

Solutio problematis arithmetici de inveniendo numero, qui per datos numeros divisus, relinquat data residua.

(Comment. VII. 1734 — 35. p. 46.)

§ 1. Reperiuntur in vulgaribus arithmeticorum libris passim hujusmodi problemata, ad quae perfecte resolvenda plus studii et sollertiae requiritur quam quidem videatur. Quamvis enim plerumque regula sit adjecta, cujus ope solutio obtineri queat, tamen ea vel est insufficiens solique casui proposito convenit, ita ut circumstantiis quaestionis parum immutatis, ea nullius amplius sit usus; vel subinde etiam solet esse falsa. Ita quadratorum magicorum constructio jam pridem ab arithmeticis est tradita; quae autem cum esset insufficiens majora ingenia Lahirii et Sauveurii ad perficiendum requisivit. Simili quoque modo ubique fere occurrit istud problema, ut inveniatur numerus, qui per 2, 3, 4, 5 et 6 divisus relinquat unitatem, per 7 vero dividi queat sine residuo: methodus vero idonea ad hujusmodi problemata solvenda nusquam exhibetur; solutio enim ibi adjecta in hunc tantum casum competit, atque tentando potius absolvitur.

§ 2. Si quidem numeri, per quos quaesitus numerus dividi debet, sunt parvi, prout in hoc exemplo, tentando non difficulter quaesitus numerus invenitur; difficillima autem foret istiusmodi solutio, si divisores propositi essent valde magni. Cum itaque ad hujus generis problemata solvenda methodus etiamnum habeatur nulla genuina, quae ad magnos divisores aeque pateat, ac ad parvos; non inutiliter operam meam collocatam esse confido, dum in hujusmodi methodum inquisivi, qua sine tentatione pro maximis etiam divisoribus talia problemata resolvi queant.

§ 3. Quo igitur, quae hac de re sum meditatus, distincte exponam, a casu incipio simplicissimo, quo unicus tantum datur divisor, numerusque quaeritur, qui per illum divisus datum relinquat residuum. Requiratur scilicet numerus z, qui per numerum a divisus relinquat p pro residuo. Hujus quidem quaestionis solutio est facillima, erit enim $z = ma + p$, denotante m numerum quemcunque integrum; interim tamen observari convenit hanc solutionem esse universalem, omnesque numeros satisfacientes complecti. Praeterea ex ea quoque intelligitur, si unus habeatur numerus satisfaciens, ex eo innumerabiles alios satisfacientes quoque posse inveniri, dum ille numerus quocunque multiplo ipsius a vel augeatur, vel si fieri potest, minuatur. Erit autem p seu $0a + p$ minimus numerus satisfaciens, hunc excipit $a + p$, quem porro sequuntur $2a + p$, $3a + p$, $4a + p$, etc. qui numeri omnes constituunt progressionem arithmeticam differentiam constantem habentem a.

§ 4. Hoc exposito sequitur casus, quo duo divisores cum suis residuis proponuntur, qui est praecipuus, et sequentes omnes in se complectitur. Nam quotcunque propositi fuerint divisores, quaestio semper ad hunc casum, quo duo tantum proponuntur, reduci poterit, quemadmodum in sequentibus monstrabo. Quaeri igitur oporteat numerum z, qui per a divisus relinquat p, per b vero divisus relinquat q; sitque numerus a major numero b. Cum ergo numerus quaesitus z ita debeat esse comparatus, ut per a divisus relinquat p, necessario in hac forma $ma + p$ continebitur, eritque idcirco $z = ma + p$. Deinde ex altera conditione, qua z per b divisus relinquere debeat

q, erit $z = nb + q$. Quamobrem, cum sit $ma + p = nb + q$, determinari debebunt numeri integri loco m et n substituendi, ut sit $ma + p = nb + q$, quibus inventis erit $ma + p$ seu $nb + q$ numerus quaesitus z.

§ 5. Quia ergo est $ma + p = nb + q$, erit $n = \frac{ma + p - q}{b}$, seu posito $p - q = v$, erit $n = \frac{ma + v}{b}$. Hanc ob rem definiri oportet numerum m, ut $ma + v$ dividi possit sine residuo per b. Quia est $a > b$, ponatur $a = \alpha b + c$; erit $n = m\alpha + \frac{mc + v}{b}$; oportet ergo ut $mc + v$ divisionem per b admittat; sunt autem α et c numeri cogniti, qui reperiuntur ex divisione ipsius a per b; erit enim α quotus et c residuum. Ponatur porro $\frac{mc + v}{b} = A$, erit $m = \frac{Ab - v}{c}$; quare numerum A inveniri oportet, ut $Ab - v$ dividi queat per c. Si eveniat, ut v per c dividi possit, operatio jam poterit finiri; sumto enim $A = 0$, erit $m = -\frac{v}{c}$ et $z = -\frac{av}{c} + p$, quae expressio, etiamsi evadat negativa, tamen ad infinitos numeros affirmativos pro z inveniendos est idonea.

§ 6. Sin autem v per c non potest dividi, quo $\frac{Ab - v}{c}$ fiat numerus integer, pono $b = \beta c + d$, seu divido b per c, dicoque quotum $= \beta$ et residuum $= d$. Quo facto erit $\frac{Ab - v}{c} = A\beta + \frac{Ad - v}{c} = m$, debebitque $\frac{Ad - v}{c}$ esse numerus integer; sit is $= B$, fiet $A = \frac{Bc + v}{d}$. Si nunc v per d dividi poterit, facio $B = 0$, eritque $A = \frac{v}{d}$ et $m = \frac{\beta v}{d}$. Sin autem v per d non est divisibile, pono porro $c = \gamma d + e$; eritque $A = B\gamma + \frac{Be + v}{d}$. Atque pono $\frac{Be + v}{d} = C$, ut sit $B = \frac{Cd - v}{e}$. Si nunc v per e dividi poterit, pono $C = 0$ eritque $B = -\frac{v}{e}$ et $A = -\frac{\gamma v}{e}$ atque $m = -\frac{\beta\gamma v}{e} - \frac{v}{e}$; sin $\frac{v}{e}$ nondum fuerit integer numerus, pono $d = \delta e + f$, eritque $B = C\delta + \frac{Cf - v}{e}$; atque facio $\frac{Cf - v}{e} = D$, ut sit $C = \frac{De + v}{f}$, ubi videndum est utrum v per f dividi possit an secus, atque in utroque casu ut supra operatio debet institui.

§ 7. Quia autem $a > b$, atque $b > c$ et $c > d$ etc. hac serie a, b, c, d, e, f, etc. continuanda perpetuo ad minores numeros devenitur, ita ut tandem ad tam parvum perveniri oporteat, qui sit pars aliquota seu divisor ipsius v. Sunt autem c, d, e, f, etc. continua residua ordinariae operationis, qua maximus communis divisor ipsarum a et b investigari solet, quam operationem hic appono

$n = \frac{ma + v}{b}$	b	a	α	$a = \alpha b + c$
$n = \frac{Ab - v}{c}$	c	b	β	$b = \beta c + d$
$A = \frac{Bc + v}{d}$	d	c	γ	$c = \gamma d + e$
$B = \frac{Cd - v}{e}$	e	d	δ	$d = \delta e + f$
$C = \frac{De + v}{f}$	f	e	ε	$e = \varepsilon f + g$
$D = \frac{Ef - v}{g}$	g	f	ζ	$f = \zeta g + h$
$E = \frac{Fg + v}{h}$	h	g	η	$g = \eta h + i$
$F = \frac{Gh - v}{i}$	i	h	ϑ	$h = \vartheta i + k$
$G = \frac{Hi + v}{k}$		k		

§ 8. Haec ergo operatio, qua ad maximum communem divisorem numerorum a et b uti solemus, eousque est continuanda, donec ad residuum perveniatur, quod dividat v. Quo invento sequenti modo investigabimus numerum m. Si v jam per b dividi poterit, fiet $m = 0$. Si v per c divisionem admittat, fiet $A = 0$ et $m = \frac{-v}{c}$. Si v per d dividatur, fiet $B = 0$ et $A = \frac{v}{d}$, atque $m = \frac{bv}{cd} - \frac{v}{c} = \frac{\beta v}{d}$ ob $b = \beta c + d$. Quo autem valores ipsius m facilius reperiantur, primo valor ipsius A per B, tum valor ipsius B per C et ita porro exprimi debet, unde nata est ista tabula:

1. $m = \frac{Ab - v}{c}$,
2. $m = \frac{Bb + \beta v}{d}$,
3. $m = \frac{Cb - v(1 + \beta\gamma)}{e}$,
4. $m = \frac{Db + v(\delta + \beta\gamma\delta + \beta)}{f}$,
5. $m = \frac{Eb - v(\delta\varepsilon + \beta\gamma\delta\varepsilon + \beta\varepsilon + \beta\gamma + 1)}{g}$,
6. $m = \frac{Fb + v(\delta\varepsilon\zeta + \beta\gamma\delta\varepsilon\zeta + \beta\varepsilon\zeta + \beta\gamma\zeta + \zeta + \delta + \beta\gamma\delta + \beta)}{h}$ etc.

De his valoribus est notandum, signa ipsius v alternari hoc modo $- + - + - +$ etc. Deinde coefficientes ipsius v hanc tenent legem:

$$\begin{array}{llllll} & \beta & \gamma & \delta & \varepsilon & \zeta \\ 1, & \beta, & \beta\gamma + 1, & \beta\gamma\delta + \delta + \beta, & \beta\gamma\delta\varepsilon + \delta\varepsilon + \beta\varepsilon + \beta\gamma + 1, & \text{etc.} \end{array}$$

cujus progressionis quisque terminus est aggregatum ex termino praecedente in indicem supra se scriptum multiplicato et termino hunc praecedente.

§ 9. Si igitur v per b dividi poterit, erit $m = 0$; si v per c dividi potest, erit $m = \frac{-v}{c}$ propter $A = 0$; si v per d dividi poterit, fiat $B = 0$; eritque $m = \frac{v}{d}\beta$. Unde sequens oritur lex:

Si est numerus integer	erit
$\frac{v}{b}$	$m = 0$
$\frac{v}{c}$	$m = -\frac{v}{c}$
$\frac{v}{d}$	$m = +\frac{v}{d}\beta$
$\frac{v}{e}$	$m = -\frac{v}{e}(\beta\gamma + 1)$
$\frac{v}{f}$	$m = +\frac{v}{f}(\beta\gamma\delta + \delta + \beta)$
$\frac{v}{g}$	$m = -\frac{v}{g}(\beta\gamma\delta\varepsilon + \delta\varepsilon + \beta\varepsilon + \beta\gamma + 1)$
$\frac{v}{h}$	$m = +\frac{v}{h}(\beta\gamma\delta\varepsilon\zeta + \delta\varepsilon\zeta + \beta\varepsilon\zeta + \beta\gamma\zeta + \beta\gamma\delta + \zeta + \delta + \beta)$ etc.

Si nunc hi ipsius m valores in aequatione $z = ma + p$ substituantur, reperietur ut sequitur:

Si est integer	erit
$\frac{v}{b}$	$z = q + \frac{bv}{b}1 = q + v$
$\frac{v}{c}$	$z = q - \frac{bv}{c}\alpha$
$\frac{v}{d}$	$z = q + \frac{bv}{d}(\alpha\beta + 1)$
$\frac{v}{e}$	$z = q - \frac{bv}{e}(\alpha\beta\gamma + \alpha + \gamma)$
$\frac{v}{f}$	$z = q + \frac{bv}{f}(\alpha\beta\gamma\delta + \alpha\beta + \alpha\delta + \gamma\delta + 1)$
$\frac{v}{g}$	$z = q - \frac{bv}{g}(\alpha\beta\gamma\delta\varepsilon + \alpha\beta\gamma + \alpha\beta\varepsilon + \alpha\delta\varepsilon + \gamma\delta\varepsilon + \alpha + \gamma + \varepsilon)$ etc.

§ 10. Ad inveniendum ergo numerum z, qui per a divisus relinquat p, et per b divisus relinquat q, posito $p - q = v$, sequentem habebimus regulam: instituatur operatio ad maximum communem divisorem inter a et b inveniendum, eaque eousque producatur, donec ad residuum perveniatur, quod sit divisor ipsius v, teneaturque quotus ex divisione ipsius v per illud residuum resultans, qui sit Q, ubi operatio abrumpatur. Deinde in serie scribantur quoti α, β, γ, etc. in hac divisione orti, ex iisque construatur nova series 1, α, $\alpha\beta + 1$, $\alpha\beta\gamma + \alpha + \gamma$, etc. quae ex illa quotorum serie formatur, atque eousque continuari debet, quousque per illam seriem fieri potest. Sub hac nova serie scribantur signa alternantia $+ - + -$ etc. ultimusque terminus cum suo signo multiplicetur per Q, atque etiam per minorem divisorem propositum b, ad factum addatur residuum q divisori b respondens. Quo facto erit aggregatum numerus quaesitus.

§ 11. Invento hoc modo uno numero satisfaciente z, ex eo statim innumerabiles alii numeri satisfacientes reperiuntur. Nam si z per a divisum p relinquit, et per b divisum q; eandem proprietatem habebunt quoque numeri $ab + z$, $2ab + z$, et $mab + z$. Multiplum quidem facti ab continuo adjici vel auferri potest, si a et b fuerint inter se numeri primi; at si a et b fuerint numeri compositi, tum etiam sufficit eorum minimum communem dividuum sumsisse; cujus multiplum quodque adjectum vel ablatum a z dabit numeros satisfacientes; ut si minimus communis dividuus fuerit M, comprehendet $mM + z$ omnes omnino numeros quaestioni satisfacientes. Quare etiamsi hoc modo saepe numeri negativi pro z inveniantur, tamen adjiciendo ad eos M vel ejus multiplum obtinebuntur numeri affirmativi. Hac ergo operatione semper minimus numerus satisfaciens invenietur, siquidem minimus communis dividuus M toties subtrahatur, quoties fieri potest.

§ 12. Quia exemplis haec operatio maxime illustrabitur, quaeramus numerum, qui per 103 divisus relinquat 87, et per 57 divisus relinquat 25. Erit ergo $a = 103$, $b = 57$, $p = 87$ et $q = 25$, atque $v = 62$; quare operationem ita instituo:

57	103	1			
	57				
	46	57	1		
		46			
		11	46	4	
			44		
			2		

$\frac{62}{2} = 31 = Q.$

1,	1,	4	
1,	1,	2,	9
+	—	+	—

Nunc est $-9.\ 31 = -279$; atque numerus quaesitus $= 25 - 57.\ 279$, qui cum fiat negativus, addo ad eum $3.\ 57.\ 103$ seu $57.\ 309$, unde invenitur $25 + 57.\ 30 = 1735$, qui est minimus numerus quaesitus; omnes vero satisfacientes continentur in hac forma $m.\ 103.\ 57 + 1735$.

§ 13. Quaeramus porro numerum, qui per 41 divisus relinquat 10, et per 29 divisus relinquat 28. In hoc exemplo compendium adhibebo, quod in aliis similibus computationibus magnam habebit utilitatem; nam cum in divisione per 29 residuum sit 28, restare quoque poterit in eadem divisione -1, si quotus unitate major accipiatur. Sumo ergo -1 pro residuo divisoris 29, eritque $a = 41$, $b = 29$, $p = 10$ et $q = -1$; unde erit $v = 11$. Operationem ergo ut ante instituo ita

```
29 | 41 | 1
   | 29 |
     12 | 29 | 2
        | 24 |
           5 | 12 | 2
             | 10 |
                2 | 5 | 2
                  | 4 |
                    1
```

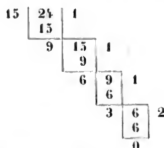
$\frac{11}{1} = 11 = Q$

1,	2,	2,	2.	
1,	1,	3,	7,	17
+	—	+	—	+

Erit ergo $+17.\ 11 = 187$; atque numerus quaesitus $= -1 + 29.\ 187$. Subtrahatur $29.\ 4.\ 41$, erit is $= -1 + 29.\ 23 = 666$. Satisfacient ergo quaestioni omnes numeri in hac forma $m.\ 41.\ 29 + 666$ contenti.

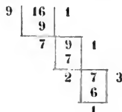
§ 14. Compendium hinc se prodit ad supra datam regulam adjiciendum, quod in hoc constat, ut, postquam numerus Q per ultimum seriei formatae terminum est multiplicatus, factum per majorem divisorem a dividatur, atque residuum loco ipsius facti adhibeatur. Scilicet hoc residuum per minorem divisorem b multiplicatum atque residuo q auctum dabit numerum quaesitum. Atque iste numerus hoc pacto inventus erit minimus, qui satisfacit. Praeterea hac divisione effici potest ut residuum prodeat affirmativum, etiamsi dividendus fuerit negativus. Ita in primo exemplo § 12 habebatur -279, qui numerus per 103 divisus, sumto quoto $= 3$ relinquit $+30$. Ex quo numerus quaesitus minimus est $= 25 + 57.\ 30 = 1735$.

§ 15. Fieri deinde etiam potest, ut hujusmodi exempla proponantur, quae solutionem omnino non admittant, uti si quaeratur numerus qui per 24 divisus relinquat 13, per 15 vero divisus relinquat 9; talis enim numerus per alteram conditionem deberet esse per 3 divisibilis, per alteram secus. Idem vero etiam ipsa regula ostendit, nunquam enim ad tale residuum, excepto 0, devenietur, quod dividat v seu 4, uti ex ipsa operatione videre est.



Hujusmodi vero exempla exhiberi non possunt, nisi divisores a et b sint numeri compositi inter se; nam si fuerint inter se primi, semper numeri quaesiti exhiberi possunt. Sin autem divisores a et b fuerint numeri compositi, atque v non dividi potuerit per maximum ipsorum a et b divisorem, tum semper problema ad absurdum deducit. Hocque est criterium, ex quo, num problema solutionem admittat, dijudicari potest, antequam operatio instituatur.

§ 16. Exposita hac methodo universali, qua omnis generis hujus problemata facile resolvi possunt, ex ea alia regula potest formari, quae quidem ad usum non est tam facilis, at simplicitatis plus in se habet. Oritur ea autem, si in valoribus supra inventis ipsius z (§ 9), loco α, β, γ, etc. eorum valores ex aequationibus $a = \alpha b + c$, $b = \beta c + d$ etc. substituantur. Nam si instituatur operatio ad maximum communem divisorem inter a et b inveniendum, ex eaque innotescant continua residua c, d, e, etc. dico fore numerum $z = q + abv\left(\frac{1}{ab} - \frac{1}{bc} + \frac{1}{cd} - \frac{1}{de} + \frac{1}{ef} - \text{etc.}\right)$, eousque hac serie continuanda, donec v per factorem aliquem denominatoris dividi queat. Uti si quaeratur numerus, qui per 16 divisus relinquat 1, et per 9 divisus relinquat 7, erit $a = 16$, $b = 9$, $p = 1$, $q = 7$, et $v = -6$. Quare



Hinc ergo erit $z = 7 - 6.9.16\left(\frac{1}{16.9} - \frac{1}{9.7} + \frac{1}{7.2}\right) = 7 - 6 + \frac{6.16}{7} - \frac{3.9.16}{7} = 1 - 3.16 = -47$, Satisfaciunt ergo omnes numeri $m.144 - 47$ seu $m.144 + 97$; eorumque minimus est 97. Superior formula generalis ipsius z etiam in hunc modum potest exprimi

$$z = p - abv\left(\frac{1}{bc} - \frac{1}{cd} + \frac{1}{de} - \frac{1}{ef} + \text{etc.}\right)$$

quae series fractionum eousque continuari debet, donec valor ipsius z fiat numerus integer.

§ 17. Considerabo nunc quosdam casus particulares, in quibus a ad b datam habeat relationem; et primo quidem sit $b = a - 1$, seu $a = b + 1$, residua vero ex divisione numeri quaesiti per a et b orta sint ut ante p et q. Erit ergo $c = 1$; ideoque per regulam postremam $z = p - av = p - ap + aq$. Quae expressio si $aq + p > ap$, dat minimum numerum quaesito satisfacientem: at si $aq + p < ap$, tum minimus numerus satisfaciens erit $a^2 - a + p - ap + aq$. Omnes vero numeri

satisfacientes in hac formula generali $ma^2 - ma + p - ap + aq$ comprehenduntur, seu etiam in ista $mb^2 + mb - bp + bq + q$. Quicquid nunc sit m, si haec quantitas dividatur per $b^2 + b$, residuum erit minimus numerus quaesito satisfaciens.

§ 18. Quemadmodum hac ratione ope residuorum datorum, quae post divisionem numeri incogniti per divisores b et $b + 1$ remanent, ipse numerus incognitus sit inveniendus, docuit Stifelius in Commentario ad Rudolfi artem Cossicam. Regula ejus ita se habet: si fuerit residuum numeri incogniti per $b + 1$ divisi p, et residuum ejusdem per b divisi q, jubet q multiplicare per $b + 1$, et p per b^2, horumque factorum aggregatum per $b^2 + b$ dividere; quod restat post divisionem, id pronunciat esse numerum quaesitum. Fluit autem haec regula ex nostra generali formula, si ponatur $m = p$, tum enim habetur $b^2 p + (b + 1) q$, quod per $b^2 + b$ divisum relinquit minimum numerum quaesitum.

§ 19. Interim tamen minori opera minimus numerus satisfaciens reperietur sequenti modo: Residuum q, quod ex divisione quaesiti numeri per b oritur, multiplicetur per $b + 1$, factumque addatur ad numerum pronicum ipsius b, puta ad $b^2 + b$, hinc subtrahatur factum ex residuo p, quod ex divisione numeri quaesiti per $b + 1$ remanet, ducto in b; si id quod restat fuerit $< b^2 + b$, erit id ipse numerus quaesitus, sin vero fuerit $> b^2 + b$, subtrahatur $b^2 + b$, eritque residuum numerus quaesitus. Ut si quaeratur numerus, qui per 100 divisus relinquat 75, et per 101 divisus 37; tum addatur 10100 ad factum ex 75 in 101 seu 7575, ut habeatur 17675, hinc subtrahatur factum ex 37 in 100 seu 3700, remanebit 13975, a quo si 10100 auferatur, prodibit 3875, qui est minimus numerus quaesitus.

§ 20. Si quaeratur numerus, qui per b divisus relinquat q, et per $nb + 1$ divisus p; erit iterum $c = 1$, atque numerus quaesitus $z = p - av = p - ap + aq = (nb + 1) q - nbp$, ob $a = nb + 1$. Atque omnes numeri satisfacientes continebuntur in hac expressione $mnb^2 + mb + (nb + 1) q - nbp$, ex qua sumto pro m numero quocunque, invenietur minimus numerus satisfaciens, si ea expressio dividatur per $nb^2 + b$; residuum enim erit minimus numerus satisfaciens.

§ 21. Casus porro notari meretur, quo residua p et q, quae oriuntur ex divisione quaesiti numeri per datos divisores a et b, sunt inter se aequalia, seu $p = q$. Hoc enim casu fit $v = 0$, ideoque invenitur numerus quaesitus $z = p$. Si igitur sit M minimus communis dividuus numerorum a et b, omnes numeri satisfacientes continebuntur in hac formula $mM + p$. Eadem plane formula quoque satisfacit, si quotcunque fuerint divisores a, b, c, d, etc. per quos singulos numerus quaesitus divisus relinquat p, si quidem M denotet omnium divisorum minimum communem dividuum. Omnes ergo numeri hujusmodi quaestionibus satisfacientes ita sunt comparati, ut per M divisi relinquant p.

§ 22. Hinc satis tritum problema, quo quaeritur numerus, qui per 2, 3, 4, 5, 6 divisus relinquat 1, per 7 vero nihil relinquat, solvi potest. Omnes enim numeri qui per 2, 3, 4, 5, 6 divisi relinquunt 1, hanc habent proprietatem ut per 60, qui numerus est minimus communis dividuus numerorum 2, 3, 4, 5 et 6, divisi relinquant 1. Problema ergo huc redit ut inveniatur numerus,

qui per 60 divisus relinquat 1, per 7 vero sit divisibilis; erit ergo $a = 60$, $b = 7$, $p = 1$, $q = 0$, et $v = 1$. Facta ergo operatione:

7 | 60 | 8
56
4 | 7 | 1
4
3 | 4 | 1
3
1

$\frac{1}{1} = 1 = Q$.
8, 1, 1.
1, 8, 9, 17.
+ — + —

Ergo $z = 0 - 119 + 420\,m$,
et si $m = 1$, erit $z = 301$.

§ 23. Majorem difficultatem habere videtur hoc problema, quo quaeritur numerus, qui per numeros 2, 3, 4, 5, 6, divisus respective relinquat numeros 1, 2, 3, 4, 5, at per 7 dividi queat, propter residua proposita inaequalia. Sed haec quaestio congruit cum hac: invenire numerum, qui per 2, 3, 4, 5, 6 divisus relinquat -1 et per 7 nihil. Illi jam conditioni satisfacit forma $60\,m - 1$; quare numerus quaeritur qui per 60 divisus -1, at per 7 nihil relinquat; fit itaque $a = 60$, $b = 7$, $p = -1$, $q = 0$, et $v = -1$, atque operatione ut ante instituta est $Q = -1$ quod in -17 ductum dat $+17$, hocque per b multiplicatum dat 119 numerum quaesitum.

§. 24. Ex his duobus exemplis apparet, quomodo hujusmodi quaestiones, in quibus quotcunque divisores proponuntur, quibus autem duo tantum residua respondent, per supra datas regulas solvi queant; statim enim quaestio ad quaestionem duorum divisorum reducitur: uti si omnia residua sunt aequalia, quaestio perinde solvitur, ac si unicus divisor fuisset propositus. At si residua sunt inaequalia, tum nihilominus repetendis his operationibus, quibus pro duobus divisoribus usi sumus, solutio poterit obtineri. Primo enim duobus divisoribus satisfieri debet, tum tertius assumitur, deinde quartus, donec omnibus erit satisfactum. Hoc vero commodissime exemplis explicabitur.

§ 25. Quaeramus igitur numerum, qui per 7 divisus relinquat 6, per 9 relinquat 7, per 11 relinquat 8, et per 17 relinquat 1. Ex his jam quatuor conditionibus sumamus duas quasque, ut duas priores, et investigemus omnes numeros iis satisfacientes Erit ergo $a = 9$, $b = 7$, $p = 7$, $q = 6$ et $v = 1$, quare operatio instituetur uti sequitur:

7 | 9 | 1
7
2 | 7 | 3
6
1

$Q = 1$.

1, 3.
1, 1, 4
+ — +

fietque $z = 6 + 1 . 4 . 7 = 34$.

Omnes ergo numeri his duabus conditionibus satisfacientes continentur in hac forma $63\,m + 34$, seu ita erunt comparati, ut per 63 divisi relinquant 34.

§ 26. Problema ergo huc est reductum, ut inveniatur numerus, qui divisus per 63 relinquat 34, per 11 relinquat 8, et per 17 relinquat 1. Harum trium conditionum sumantur duae priores eritque $a = 63$, $b = 11$, $p = 34$, $q = 8$, et $v = 26$, unde fluit sequens operatio:

11	63	5			
	55				
	8	11	1		
		8			
		3	8	2	
			6		
			2		

$Q = \frac{26}{2} = 13.$

5, 1, 2.

1, 5, 6, 17. Ergo $z = m.63.11 + 8 - 13.17.11.$

$+ \quad - \quad + \quad -$

Quo minimus numerus satisfaciens reperiatur, ponatur $m = 4$; erit $z = 8 + 31.11 = 349$. Omnes ergo numeri satisfacientes in hac continentur forma $693m + 349$, seu hanc habebunt proprietatem, ut per 693 divisi relinquant 349.

§ 27. Problema ergo tandem huc est reductum, ut definiatur numerus, qui per 693 divisus relinquat 349, et per 17 divisus relinquat 1. Facio ergo $a = 693$, $b = 17$, $p = 349$, $q = 1$, et $v = 348$, sequentemque juxta data praecepta instituo operationem:

17	693	41
	697	
	-4	

$Q = \frac{348}{-4} = -87.$

41.

1, 41. $\quad z = 693.17.m + 1 + 41.87.17.$

$+ \quad -$

Quo minimus numerus satisfaciens prodeat, pono $m = -5$, eritque $z = 1 + 102.17 = 1735$, qui est minimus numerus quatuor praescriptis conditionibus satisfaciens. Omnes autem qui satisfaciunt, hac continentur formula $11781\,m + 1735$. Ex hoc exemplo ergo abunde intelligitur, quomodo omnes hujusmodi quaestiones sint resolvendae.

§ 28. Pertinet huc solutio problematis chronologici satis cogniti, quam, prout ex his regulis inveni, apponam, in quo annus a Christo nato quaeritur, ex datis cyclis solis et lunae una cum indictione Romana illius anni. Cum enim cyclus solis sit residuum, quod oritur divisione numeri anni novenario aucti per 28; cyclus vero lunae sit residuum, quod oritur divisione numeri anni unitate aucti per 19; indictio vero Romana sit residuum, quod oritur, si numerus anni ternario auctus per 15 dividatur, sequens prodiit solutio. Sit p cyclus solis, q cyclus lunae, et r indictio Romana; multiplicetur p per 4845; q per 4200, et r per 6916, haec tria producta cum numero 3267 in unam summam conjiciantur, eaque dividatur per 7980; quod remanebit residuum erit numerus anni quaesiti. Si annus periodi Julianae requiratur, tum operatio eodem modo instituatur, nisi quod numerus 3267 negligi debet; quae est regula jam passim tradita.

§ 29. Multam quidem operam requirit solutio pro pluribus divisoribus, si quidem problema continuo ad casum, quo divisorum numerus unitate minuitur, ut in praecedente exemplo fecimus,

reducitur; at ex ea ipsa operatione facilior multoque brevior via sese prodit, qua statim proposita quaestio, quotcunque etiam fuerint divisores, ad casum duorum divisorum reduci potest; quae regula ita se habet: Inveniendus sit numerus, qui per divisores a, b, c, d, e, quos numeros inter se primos esse pono, divisus relinquat respective haec residua p, q, r, s, t. Huic quaestioni satisfacit iste numerus $Ap + Bq + Cr + Ds + Et + mabcde$, in qua expressione A est numerus, qui per factum $bcde$ divisus nihil relinquat, per a vero divisus relinquat unitatem; B est numerus, qui per $acde$ divisus relinquat nihil, per b vero unitatem; C est numerus, qui per $abde$ divisus nihil relinquat, per c vero unitatem; D est numerus, qui per $abce$ divisus nihil relinquat, per d vero unitatem; atque E est numerus, qui per $abcd$ divisus nihil relinquat, per e vero unitatem; qui ergo numeri per regulam pro duobus divisoribus datam inveniri possunt.



IV.

Theorematum quorundam ad numeros primos spectantium demonstratio.

(Comment. VIII. 1736. p. 141.)

§ 1. Plurima quondam a Fermatio theoremata arithmetica sed sine demonstrationibus in medium sunt prolata, in quibus, si vera essent, non solum eximiae numerorum proprietates continerentur, verum etiam ipsa numerorum scientia, quae plerumque analyseos limites excedere videtur, vehementer esset promota. Quamvis autem iste insignis Geometra de pluribus, quae proposuit, theorematibus asseruerit se ea vel demonstrare posse, vel saltem de eorum veritate esse certum: tamen nusquam, quantum mihi constat, demonstrationes exposuit. Quin potius Fermatius videtur maximam theorematum suorum numericorum partem per inductionem esse assecutus, quippe quae via fere unica ad hujusmodi proprietates eruendas patere videatur. At vero quam parum inductionibus in hoc negotio tribui possit, pluribus exemplis possem declarare; ex quibus autem unicum ab ipso Fermatio desumtum attulisse sufficiat. Loquor nimirum de illo theoremate, cujus falsitatem jam aliquot ab hinc annis ostendi, quo Fermatius asserit omnes numeros hac forma $2^{2^n}+1$ comprehensos esse numeros primos*). Ad veritatem autem hujus propositionis evincendam inductio omnino sufficere videatur. Nam praeterquam quod omnes isti numeri minores quam 100000 sint revera primi, demonstrari etiam facile potest nullum numerum primum, 600 non excedentem hanc formulam $2^{2^n}+1$, quantumvis magnus etiam numerus pro n substituatur, metiri. Cum tamen nihilominus constet hanc propositionem veritati non esse consentaneam, facile intelligitur, quantum inductio in hujusmodi speculationibus valeat.

§ 2. Hanc ob rationem omnes hujusmodi numerorum proprietates, quae sola inductione nituntur, tam diu pro incertis habendas esse arbitror, donec illae vel apodicticis demonstrationibus muniantur, vel omnino refellantur. Non plus etiam illis theorematibus, quae ego ipse illi schediasmati, in quo de memorato theoremate Fermatiano numerisque perfectis tractavi, subjeci, fidendum esse censerem, si tantum inductionibus, qua via quidem sola tum temporis ad eorum cognitionem perveni, niterentur. Nunc vero, postquam peculiari methodo demonstrationes horum theorematum firmissimas sum adeptus, de veritate eorum non amplius est dubitandum. Quocirca tam ad veritatem illorum theorematum ostendendam, quam ad methodum ipsam, quae forte etiam in aliis numerorum investigationibus utilitatem afferre poterit, in hac dissertatione meas demonstrationes explicare constitui.

§ 3. Propositio autem, quam hic demonstrandum suscepi, est sequens:

Significante p numerum primum, formula $a^{p-1}-1$ semper per p dividi poterit, nisi a per p dividi queat.

Ex hac enim propositione demonstrata sponte reliquorum theorematum veritas fluit. Casum quidem formulae propositae, quo est $a=2$, jam ab aliquo tempore demonstratum dedi**): attamen tum de-

*) Conf. comment. I. pag. 1 et seq. **) l. c. pag. 2.

monstrationem ad generalem formulam extendere non licuit. Quamobrem primo hujus casus probationem afferre conveniet, quo transitus ad generaliora eo facilior reddatur. Demonstranda igitur erit sequens propositio:

Significante p numerum primum imparem quemcunque, formula $2^{p-1}-1$ semper per p dividi poterit.

Demonstratio. Loco 2 ponatur $1+1$, eritque

$$(1+1)^{p-1}=1+\frac{p-1}{1}+\frac{(p-1)(p-2)}{1.\ \ 2}+\frac{(p-1)(p-2)(p-3)}{1.\ \ 2.\ \ 3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1.\ \ 2.\ \ 3.\ \ 4}+\text{etc.},$$

cujus seriei terminorum numerus est $=p$ et proinde impar. Praeterea quilibet terminus, quamvis habeat fractionis speciem, dabit numerum integrum; quisque enim numerator, uti satis constat, per suum denominatorem dividi potest. Demto igitur seriei termino primo 1, erit

$$(1+1)^{p-1}-1=2^{p-1}-1=\frac{p-1}{1}+\frac{(p-1)(p-2)}{1.\ \ 2}+\frac{(p-1)(p-2)(p-3)}{1.\ \ 2.\ \ 3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1.\ \ 2.\ \ 3.\ \ 4}+\text{etc.},$$

quorum numerus est $=p-1$ et propterea par. Colligantur igitur bini quique termini in unam summam, quo terminorum numerus fiat duplo minor, erit

$$2^{p-1}-1=\frac{p(p-1)}{1.\ \ 2}+\frac{p(p-1)(p-2)(p-3)}{1.\ \ 2.\ \ 3.\ \ 4}+\frac{p(p-1)(p-2)(p-3)(p-4)(p-5)}{1.\ \ 2.\ \ 3.\ \ 4.\ \ 5.\ \ 6}+\text{etc.},$$

cujus seriei ultimus terminus, ob p numerum imparem, erit $\frac{p(p-1)(p-2)\ldots\ldots\ldots\ldots 2}{1.\ \ 2.\ \ 3\ldots\ldots\ldots\ldots(p-1)}=p$. Apparet autem singulos terminos per p esse divisibiles, nam, cum p sit numerus primus et major quam ullus denominatorum factor, nusquam divisione tolli poterit. Quamobrem si fuerit p numerus primus impar, per illum semper $2^{p-1}-1$ dividi poterit. Q. E. D.

Aliter. Si $2^{p-1}-1$ per numerum primum p dividi potest, dividi quoque poterit ejus duplum 2^p-2 et vicissim. At est $2^p=(1+1)^p=1+\frac{p}{1}+\frac{p(p-1)}{1.\ \ 2}+\frac{p(p-1)(p-2)}{1.\ \ 2.\ \ 3}\ldots\ldots+\frac{p}{1}+1$. Quae series terminis primo et ultimo truncata dat

$$\frac{p}{1}+\frac{p(p-1)}{1.\ \ 2}+\frac{p(p-1)(p-2)}{1.\ \ 2.\ \ 3}+\ldots\ldots+\frac{p(p-1)}{1.\ \ 2}+p=2^p-2.$$

Perspicuum autem est istius seriei quemvis terminum per p esse divisibilem, si quidem p fuerit numerus primus. Quamobrem etiam semper 2^p-2 per p, et propterea quoque $2^{p-1}-1$ per p dividi poterit, nisi sit $p=2$. Q. E. D.

§ 4. Cum igitur $2^{p-1}-1$ per numerum primum imparem p dividi queat, facile intelligitur per p quoque dividi posse hanc formulam $2^{m(p-1)}-1$, denotante m numerum quemcunque integrum. Quare sequentes formulae quoque omnes $4^{p-1}-1$, $8^{p-1}-1$, $16^{p-1}-1$ etc. per numerum primum p dividi poterunt. Demonstrata igitur est veritas theorematis generalis pro omnibus casibus, quibus a est quaevis binarii potestas, et p quicunque numerus primus praeter binarium.

§ 5. Demonstrato nunc hoc theoremate, ejus ope sequens quoque demonstrabimus

Theorema. Denotante p numerum primum quemcunque praeter 3, per illum semper haec formula $3^{p-1}-1$ dividi poterit.

Demonstratio. Si $3^{p-1}-1$ per numerum primum p excepto 3 dividi potest, tum 3^p-3 per p dividi poterit, quoties p fuerit numerus primus quicunque, et vicissim. Est vero

$$3^p=(1+2)^p=1+\frac{p}{1}\cdot 2+\frac{p(p-1)}{1.\ \ 2}\cdot 4+\frac{p(p-1)(p-2)}{1.\ \ 2.\ \ 3}\cdot 8\ \ldots\ldots+\frac{p}{1}\cdot 2^{p-1}+2^p,$$

cujus seriei singuli termini, praeter primum et ultimum, per p dividi poterunt, si quidem p fuerit numerus primus. Per p igitur dividi potest ista formula $3^p - 2^p - 1$, quae aequalis est huic $3^p - 3 - 2^p + 2$. At $2^p - 2$ semper per p numerum primum dividi potest; ergo etiam $3^p - 3$. Quare $3^{p-1} - 1$ semper per p dividi potest, quoties p fuerit numerus primus excepto 3. Q. E. D.

§ 6. Eodem modo ulterius progredi liceret ab hoc ipsius a valore ad sequentem unitate majorem. Sed quo demonstrationem generalis theorematis magis concinnam magisque genuinam efficiam, sequens praemitto

Theorema. Denotante p numerum primum, si $a^p - a$ per p dividi potest, tum per idem p quoque formula $(a+1)^p - a - 1$ dividi poterit.

Demonstratio. Resolvatur $(1 + a)^p$ consueto more in seriem, erit

$$(1 + a)^p = 1 + \frac{p}{1} a + \frac{p(p-1)}{1.\ 2} a^2 + \frac{p(p-1)(p-2)}{1.\ 2.\ \ 3} a^3 + \cdots\cdots + \frac{p}{1} a^{p-1} + a^p;$$

cujus seriei singuli termini per p dividi possunt, praeter primum et ultimum, si quidem p fuerit numerus primus. Quamobrem $(1 + a)^p - a^p - 1$ divisionem per p admittet; haec autem formula congruit cum hac $(1 + a)^p - a - 1 - a^p + a$. At $a^p - a$ per hypothesin per p dividi potest, ergo et $(1 + a)^p - a - 1$. Q. E. D.

§ 7. Cum igitur, posito quod $a^p - a$ per p numerum primum dividi queat, per p quoque haec formula $(a+1)^p - a - 1$ divisionem admittat; sequitur etiam $(a + 2)^p - a - 2$, item $(a + 3)^p - a - 3$, et generaliter $(a + b)^p - a - b$ per p dividi posse. Posito autem $a = 2$, quia $2^p - 2$, uti jam demonstravimus, per p dividi potest, perspicuum est formulam $(b + 2)^p - b - 2$ divisionem per p admittere debere, quicunque integer numerus loco b substituatur. Metietur ergo p formulam $a^{p-1} - 1$, nisi fuerit $a = p$ vel multiplo ipsius p. Atque haec est demonstratio generalis theorematis, quam tradere suscepi.

V.

Theorematum quorundam arithmeticorum demonstrationes.

(Comment. X. 1738. p. 125.)

Theoremata arithmetica, cujusmodi Fermatius aliique plurima detexerunt, eo majore attentione sunt digna, quo magis eorum veritas est abscondita, et demonstratu difficilis. Fermatius quidem satis magnam talium theorematum copiam reliquit, nusquam autem demonstrationes exposuit, etiamsi firmiter asserat, sibi de eorum veritate certissime constare. Maxime igitur dolendum est ejus scripta adeo periisse, ut etiamnum omnes demonstrationes ignorentur. Similis quoque est ratio propositionum in vulgus notarum, quibus neque summam neque differentiam duorum biquadratorum quadratum constituere posse asseritur; quamvis enim de earum veritate nemo dubitet, tamen nusquam exstat demonstratio, quantum mihi quidem constat, rigida, praeter libellum quemdam a Freniclio olim editum, cujus titulus est *Traité des triangles rectangles en nombres.* Demonstrat autem hic autor, inter alia, in nullo triangulo rectangulo, cujus latera rationalibus exprimuntur numeris, aream posse esse quadratum, unde facile veritas memoratarum propositionum de summa et differentia duorum biquadratorum deducitur. Sed ista demonstratio tantopere proprietatibus triangulorum est involuta, ut nisi summa attentio adhibeatur, vix perspicue intelligi possit. Hanc ob rem operae pretium fore arbitror, si harum propositionum demonstrationes a triangulis rectangulis abstraxero, easque analytice et clare proposuero. Eo majorem autem hoc meum institutum afferret utilitatem, quo plura alia theoremata multo difficiliora ex iis elici possunt. Huc scilicet pertinet theorema illud celebre Fermatii, quo statuit, nullum numerum trigonalem esse posse biquadratum praeter unitatem, cujus demonstrationem ex illis formare mihi contigit. Eo difficilior autem ista demonstratio videtur, cum propositio exceptioni sit obnoxia, atque tantum ad numeros integros pertineat; numeris enim fractis infinitis modis effici potest, ut $\frac{x(x+1)}{2}$ fiat biquadratum. Ad hoc igitur aliaque nonnulla theoremata demonstranda necesse erit lemmata quaedam praemittere, quibus sequentes demonstrationes innituntur; ante autem monuisse oportet, perpetuo omnes litteras mihi numeros integros designare.

Lemma 1. Factum ex duobus pluribusve numeris inter se primis nec quadratum nec cubus nec ulla alia potestas esse potest, nisi singuli factores sint quadrata vel cubi vel ejusmodi aliae potestates.

Demonstratio hujus lemmatis facilis est atque ab Euclide jam est tradita, ita ut superfluum foret eam hic exponere.

Lemma 2. Si a^2+b^2 fuerit quadratum, atque a et b sint numeri inter se primi, erit $a=pp-qq$ et $b=2pq$, existentibus p et q numeris inter se primis, altero pari altero impari.

Demonstratio. Quia est a^2+b^2 quadratum, ponatur ejus radix $=a+\frac{bq}{p}$, ubi fractionem $\frac{q}{p}$ in minimis terminis pono expressam, ita ut p et q sint numeri inter se primi. Facta autem

aequatione erit $a^2 + b^2 = a^2 + \frac{2abq}{p} + \frac{bbqq}{pp}$, unde fit $a:b = pp - qq : 2pq$. Numeri autem $pp - qq$ et $2pq$ inter se vel primi sunt, vel communem habent divisorem 2. Illo igitur casu, quo $pp - qq$ et $2pq$ sunt numeri inter se primi, quod accidit, si numerorum p et q alter fuerit par, alter impar, necesse est ut sit $a = pp - qq$ et $b = 2pq$: quia a et b numeri ponuntur inter se primi. Casu autem, quo numeri $pp - qq$ et $2pq$ communem divisorem habent 2; quod erit, si numerorum p et q uterque fuerit impar, (uterque enim par esse nequit, quia inter se ponuntur primi), erit $a = \frac{pp - qq}{2}$ et $b = pq$. Ponatur autem $p + q = 2r$ et $p - q = 2s$, erunt r et s numeri inter se primi, eorumque alter par alter impar, unde fit $a = 2rs$ et $b = rr - ss$; quae expressio, quia cum priori congruit, indicat si $aa + bb$ fuerit quadratum, et numeri a et b sint inter se primi, alterum eorum esse differentiam duorum quadratorum inter se primorum, quorum alter par est, alter impar, alterum vero numerum aequari duplici facto ex radicibus istorum quadratorum. Hoc est esse $a = pp - qq$ et $b = 2pq$, existentibus p et q numeris inter se primis, altero pari altero impari. Q. E. D.

Coroll. 1. Si ergo summa duorum quadratorum inter se primorum fuerit quadratum, alterum quadratum par sit necesse est, alterum vero impar: ex quo sequitur summam duorum quadratorum imparium non posse esse quadratum.

Coroll. 2. Si ergo $aa + bb$ est quadratum, numerorum a et b alter, puta a, erit impar, alter b vero par. Impar vero a erit $= pp - qq$, et par $b = 2pq$.

Coroll. 3. Quia porro numerorum p et q alter est par alter impar, erit b numerus pariter par, seu per 4 divisibilis. Deinde si nec p nec q fuerit per 3 divisibilis, necesse est ut vel $p - q$, vel $p + q$ divisionem per 3 admittat. Unde sequitur alterum numerorum a et b, quorum quadratorum summa facit quadratum, esse per 3 divisibilem.

Coroll. 4. Cum sit $a = pp - qq$ et $b = 2pq$, si $aa + bb$ constituat quadratum, facile intelligitur numeros p et q minores esse quam a et b. Quoniam enim est $a = (p + q)(p - q)$, erit $a > p + q$, nisi $p - q$ sit $= 1$; atque ob $b = 2pq$, erit b major quam p vel q. Potiori ergo ratione numeri a et b majores erunt quam numeri p et q. Fieret quidem $a = 0$, si foret $p = q$, sed hic casus locum non habet, quia p et q ponuntur numeri inter se primi, eorumque alter par alter impar.

Scholion. In demonstratione hujus lemmatis ex analogia $a:b = pp - qq : 2pq$ ideo sequitur esse $a = pp - qq$ et $b = 2pq$, quia a et b sunt numeri inter se primi, pariterque numeri $pp - qq$ et $2pq$. Si enim fuerit $a:b = c:d$, atque tam numeri a et b quam numeri c et d sint primi inter se, necesse est ut sit $a = c$ et $b = d$; prout facile ex natura proportionum constat.

Lemma 3. Si fuerit $aa - bb$ quadratum, existentibus a et b numeris inter se primis, erit $a = pp + qq$ et vel $b = pp - qq$ vel $b = 2pq$, ubi numeri p et q sunt inter se primi, eorumque alter par alter impar.

Demonstratio. Quia $aa - bb$ est quadratum, ponatur $a^2 - b^2 = c^2$, eritque $a^2 = b^2 + c^2$, atque b et c numeri inter se primi. Cum igitur, per coroll. 1 lemmatis praecedentis, numerorum b et c alter par sit alter impar, necesse est ut a sit numerus impar; b vero vel par erit vel impar.

Sit primo b impar et c par, erit per lemma praecedens, $b = pp - qq$ et $c = 2pq$, existentibus p et q numeris inter se primis altero pari altero impari. Hinc autem fit $a = pp + qq$. At si b

fuerit par et c impar, erit $b = 2pq$ et $c = pp - qq$, unde denuo fit $a = pp + qq$. Quocirca si $aa - bb$ fuerit quadratum, erit $a = pp + qq$, atque vel $b = pp - qq$ vel $b = 2pq$. Q. E. D.

Coroll. 1. Si ergo differentia duorum quadratorum est numerus quadratus, majus quadratum debet esse numerus impar, si quidem illa quadrata inter se fuerint numeri primi.

Coroll. 2. Simili porro modo intelligitur numeros p et q minores esse quam numeros a et b, cum sit $a = pp + qq$ atque b vel $= pp - qq$ vel $= 2pq$.

Coroll. 3. Si fuerit $aa - bb = cc$, unus numerorum a, b, c semper per 5 divisibilis existit. Nam cum sit $a = pp + qq$, $b = pp - qq$ et $c = 2pq$; vel alter numerorum p et q per 5 divisibilis est vel neuter; illo autem casu fit c divisibile per 5. Hoc vero casu erunt pp et qq numeri ejusmodi formae $5n \pm 1$, ergo vel $pp - qq$ vel $pp + qq$ per 5 divisibile erit.

Theorema 1. Summa duorum biquadratorum ut $a^4 + b^4$ non potest esse quadratum, nisi alterum biquadratum evanescat.

Demonstratio. In theoremate hoc demonstrando ita versabor, ut ostendam, si uno casu fuerit $a^4 + b^4$ quadratum, quantumvis etiam magni fuerint numeri a et b, tum continuo minores numeros loco a et b assignari posse, atque tandem ad minimos numeros integros perveniri oportere. Cum autem in minimis numeris tales non dentur, quorum biquadratorum summa quadratum constitueret, concludendum erit nec inter maximos numeros tales exstare. Ponamus ergo $a^4 + b^4$ esse quadratum, atque a et b inter se esse numeros primos; nisi enim primi forent, per divisionem ad primos reduci possent. Sit a numerus impar, b vero par, quia necessario alter par alter impar esse debet. Erit ergo $aa = pp - qq$ et $bb = 2pq$, numerique p et q inter se erunt primi, eorumque alter par alter impar. Cum autem sit $aa = pp - qq$, necesse est ut p sit numerus impar, quia alias $pp - qq$ quadratum esse non posset. Erit ergo p numerus impar et q numerus par. Quia porro $2pq$ quadratum esse debet, necesse est, ut tam p quam $2q$ sit quadratum, quia p et $2q$ sunt numeri inter se primi. Ut vero $pp - qq$ sit quadratum, necesse est, ut sit $p = mm + nn$ et $q = 2mn$; existentibus iterum m et n numeris inter se primis eorumque altero pari altero impari. Sed quoniam $2q$ quadratum est, erit $4mn$ seu mn quadratum; unde tam m quam n quadrata erunt. Posito ergo $m = xx$ et $n = yy$, erit $p = m^2 + n^2 = x^4 + y^4$, quod quadratum pariter esse deberet. Hinc ergo sequitur si $a^4 + b^4$ foret quadratum, tum quoque $x^4 + y^4$ fore quadratum; manifestum autem est numeros x et y longe minores fore quam a et b. Pari igitur via ex biquadratis $x^4 + y^4$ denuo minora orientur, quorum summa esset quadratum, atque pergendo ad minima tandem biquadrata in integris perveniretur. Cum ergo non dentur minima biquadrata, quorum summa efficeret quadratum, palam est nec in maximis numeris talia dari. Si autem in uno biquadratorum pari alterum sit $= 0$, in omnibus reliquis paribus alterum evanescet, ita ut hinc nulli novi casus oriantur. Q. E. D.

Coroll. 1. Cum igitur summa duorum biquadratorum non posset esse quadratum, multo minus duo biquadrata conjuncta biquadratum efficere poterunt.

Coroll. 2. Quamquam demonstratio haec tantum ad numeros integros pertinet, tamen etiam per eam conficitur, ne in fractis quidem duo biquadrata exhiberi posse, quorum summa esset qua-

dratum. Nam si $\frac{a^4}{m^4} + \frac{b^4}{n^4}$ foret quadratum, tum quoque in integris esset $a^4 n^4 + b^4 m^4$ quadratum, quod fieri nequit, per ipsam demonstrationem.

Coroll. 3. Ex eadem demonstratione colligere licet, non dari ejusmodi numeros p et q, ut p, $2q$ et $pp - qq$ sint quadrata, si enim tales existerent, tum haberentur valores pro a et b, qui redderent $a^4 + b^4$ quadratum, foret namque $a = \sqrt{(pp - qq)}$ et $b = \sqrt{2pq}$.

Coroll. 4. Positis ergo $p = xx$ et $2q = 4yy$, erit $pp - qq = x^4 - 4y^4$. Fieri ergo omnino nequit ut $x^4 - 4y^4$ sit quadratum. Neque igitur $4x^4 - y^4$ quadratum esse poterit, foret enim quadratum $16x^4 - 4y^4$, qui casus ob $16x^4$ biquadratum ad priorem recidit.

Coroll. 5. Sequitur hinc etiam $ab(a^2 + b^2)$ quadratum nunquam esse posse. Ob factores enim a, b, $a^2 + b^2$ inter se primos, singulos quadrata esse oporteret, quod fieri nequit.

Coroll. 6. Similiter tales etiam numeri inter se primi a et b non dabuntur, qui producerent $2ab(aa - bb)$ quadratum. Sequitur hoc ex coroll. 3, ubi monstratum est non dari numeros p et q, ut essent p, $2q$, $pp - qq$ quadrata. Haec omnia autem quoque valent pro numeris inter se non primis atque adeo fractis, per coroll. 2.

Theorema. 2. Differentia duorum biquadratorum ut $a^4 - b^4$ non potest esse quadratum, nisi sit vel $b = 0$ vel $b = a$.

Demonstratio. Theorema hoc pari modo demonstrabo quo praecedens. Sint igitur biquadrata jam ad minores terminos reducta, atque ponamus $a^4 - b^4$ esse quadratum: erit a numerus impar, b vero vel par erit vel impar.

Casus I. Sit primo b numerus par, erit $a^2 = pp + qq$ et $b^2 = 2pq$, existentibus p et q inter se primis, eorumque altero p pari altero q impari. Ob $b^2 = 2pq$, debebunt ergo $2p$ et q esse quadrata. Quia porro $pp + qq$ ipsi a^2 aequatur, erit $q = mm - nn$ et $p = 2mn$, existentibus m et n numeris inter se primis. Cum autem $2p$ sit quadratum, erit $4mn$, hoc est mn quadratum; adeoque m et n sigillatim quadrata. Factis ergo $m = x^2$ et $n = y^2$, fiet $q = x^4 - y^4$, ubi cum numerorum m et n alter sit par alter impar, erit quoque numerorum x et y alter par alter impar. At ob q quadratum, quadratum erit $x^4 - y^4$, ubi x erit numerus impar, y vero par. Quocirca si fuerit $a^4 - b^4$ quadratum, quadratum quoque erit $x^4 - y^4$, existentibus x et y longe minoribus quam a et b. Cum ergo in minimis numeris non dentur duo biquadrata, differentiam quadratam habentia, nec in maximis dabuntur, saltem casu, quo minus biquadratum est numerus par, Q. E. unum —

Casus II. Sit nunc b numerus impar, eritque $aa = pp + qq$ et $bb = pp - qq$; existentibus p et q numeris inter se primis, eorumque altero pari altero impari. Quia vero $pp - qq$ est quadratum, erit p numerus impar, et propterea q par. Ductis autem a^2 et b^2 in se invicem, prodibit $a^2b^2 = p^4 - q^4$, quae expressio, per casum primum, quadratum esse, ideoque ipsi a^2b^2 aequari non potest. Differentia ergo duorum biquadratorum nullo modo esse potest quadratum, nisi vel ambo sint aequalia, vel minus $= 0$. Q. E. alterum D.

Coroll. 1. Cum sit $a^2 = pp + qq$ et $b^2 = 2pq$ itemque $q = mm - nn$ et $p = 2mn$, atque porro $m = x^2$ et $n = y^2$, erit $a^2 = (x^4 + y^4)^2$ et $b^2 = 4x^2y^2(x^4 - y^4)$. Ex quo habebitur $a = x^4 + y^4$ et $b = 2xy\sqrt{(x^4 - y^4)}$.

Coroll. 2. Si ergo in numeris exiguis x et y darentur tales, quorum biquadratorum differentia constitueret quadratum; tum ex iis statim multo majores numeri eadem proprietate gaudentes a et b inveniri possent.

Coroll. 3. Hinc clarius perspicitur casum, quo biquadrata vel sint aequalia, vel alterum $= 0$, novos casus non praebere, facto enim vel $x = y$ vel $y = 0$, fit simul $b = 0$, unde vis demonstrationis eo magis percipitur.

Coroll. 4. Ex demonstratione porro sequitur non dari numeros p et q ejus indolis, ut essent $2p$, q et $pp + qq$ quadrata. Posito ergo $2p = 4xx$ et $q = yy$, non poterit esse quadratum ista forma $4x^4 + y^4$.

Coroll. 5. Ex his formulis quoque sequitur, nec $ab(aa - bb)$ nec $2ab(aa + bb)$ unquam fieri posse quadrata, id quod non solum valet, si a et b sint numeri inter se primi, sed etiam si compositi atque adeo fracti. Fractiones enim ejusmodi facile ad integros, atque integri ad numeros inter se primos reducuntur.

Coroll. 6. In his igitur duabus propositionibus evictum est, sequentes novem expressiones nunquam fieri posse quadrata:

I.	$a^4 + b^4$	VI.	$a^4 - b^4$
II.	$a^4 - 4b^4$	VII.	$4a^4 + b^4$
III.	$4a^4 - b^4$	VIII.	$ab(aa - bb)$
IV.	$ab(aa + bb)$	IX.	$2ab(aa + bb)$
V.	$2ab(aa - bb)$	X.	$2a^4 \pm 2b^4$

decimam expressionem ideo adjeci, quia ejus veritas mox demonstrabitur.

Theorema 3. Summa duorum biquadratorum bis sumta, ut $2a^4 + 2b^4$ quadratum esse nequit nisi sit $a = b$.

Demonstratio. Pono primo a et b numeros esse inter se primos, nam nisi tales essent, formula per divisionem eo reduci posset. Facile autem perspicitur, utrumque numerum a et b esse debere imparem, si enim alter par esset, tum fieret $2a^4 + 2b^4$ numerus impariter par, qui quadratum esse nequit. Porro haec forma congruit cum ista $(aa + bb)^2 + (aa - bb)^2$, quam ideo demonstrari oportet quadratum esse non posse, nisi sit $a = b$. At ob a et b numeros impares, erunt $a^2 + b^2$ et $a^2 - b^2$ numeri pares, ille quidem impariter, hic vero pariter par. Perventum ergo est ad hanc formam $\left(\frac{aa + bb}{2}\right)^2 + \left(\frac{aa - bb}{2}\right)^2$, in qua $\frac{aa + bb}{2}$ et $\frac{aa - bb}{2}$ sint numeri inter se primi, ille impar, iste vero par; quamobrem si forma proposita esset quadratum, foret $\frac{aa + bb}{2} = pp - qq$ et $\frac{aa - bb}{2} = 2pq$, unde reperitur $a^2 = pp + 2pq - qq$ et $b^2 = pp - 2pq - qq$, quarum expressionum differentia est $4pq = aa - bb$; ideoque erit $a + b = \frac{2mp}{n}$ et $a - b = \frac{2nq}{m}$; unde $a = \frac{mp}{n} + \frac{nq}{m}$ et $b = \frac{mp}{n} - \frac{nq}{m}$. Facta autem hac substitutione erit

$$\frac{mm}{nn}pp + \frac{nn}{mm}qq = pp - qq \quad \text{atque} \quad \frac{pp}{qq} = \frac{nn(mm + nn)}{mm(nn - mm)} = \frac{nn(n^4 - m^4)}{mm(nn - mm)^2}.$$

Oporteret ergo esse quadratum $n^4 - m^4$, quod per praecedens theorema fieri nequit Q. E. D.

Coroll. 1. Si ergo a et b fuerint numeri impares, etiam $2ab(aa+bb)$ nequit esse quadratum; deberent enim a, b et $2aa+2bb$ esse quadrata, quod per hoc theorema fieri nequit.

Coroll. 2. Demonstratio ergo etiam formari potuisset ex formula nona $2ab(aa+bb)$, sed ibi numerorum a et b alter positus erat par, alter impar, quod etiam si nihil impediret, tamen praestabat peculiarem dare demonstrationem.

Coroll. 3. Hac igitur demonstratione ipsa formulae nonae veritas magis confirmatur, cum hinc jam constet $2ab(aa+bb)$ quadratum esse non posse, etiamsi numeri a et b ambo sint impares.

Coroll. 4. Brevius vero etiam veritas hujus theorematis ostendi potest, ex forma $(a^2+b^2)^2+(a^2-b^2)^2$, quae ideo quadratum esse nequit, quia $(a^2+b^2)^2-(a^2-b^2)^2$ est quadratum. Fieri autem nequit, ut summa duorum quadratorum sit quadratum, si eorundem quadratorum differentia fuerit quadratum, si enim tam $pp+qq$, quam $pp-qq$ foret quadratum, quadratum esset p^4-q^4, quod fieri nequit.

Coroll. 5. Simili modo $a^4-6aabb+b^4$ quadratum esse nequit. Est enim

$$a^4-6aabb+b^4=(aa-bb)^2-4aabb,$$

quae est differentia ejusmodi quadratorum, quorum summa facit quadratum.

Coroll. 6. Atque pari modo $a^4+6a^2b^2+b^4$ quadratum esse nequit, quia est $=(a^2+b^2)^2+4aabb$, quorum quadratorum summa quadratum esse nequit, quia eorundem differentia $(a^2+b^2)^2-4aabb$ est quadratum.

Theorema 4. Duplum differentiae duorum biquadratorum, ut $2a^4-2b^4$ quadratum esse nequit, nisi sit $a=b$.

Demonstratio. Ponamus a et b numeros inter se primos et $2a^4-2b^4$ esse quadratum; erunt a et b numeri impares. Foret ergo $2(a-b)(a+b)(aa+bb)$ quadratum, ideoque etiam ejus pars decima sexta, seu $\left(\frac{a-b}{2}\right)\left(\frac{a+b}{2}\right)\left(\frac{aa+bb}{2}\right)$; qui factores cum sint inter se primi, singuli esse deberent quadrata. Sit ergo $\frac{a-b}{2}=pp$ et $\frac{a+b}{2}=qq$, erit $a=pp+qq$ et $b=qq-pp$, unde fit $\frac{aa+bb}{2}=p^4+q^4$. Cum igitur p^4+q^4 quadratum esse nequeat, etiam $\frac{aa+bb}{2}$, ideoque $2a^4-2b^4$ quadratum esse nequit. Q. E. D.

Theorema 5. Neque $ma^4-m^3b^4$ neque $2ma^4-2m^3b^4$ potest esse quadratum.

Demonstratio. Ponamus a et b esse numeros inter se primos, atque m numerum esse nec quadratum nec per quadratum divisibilem: si enim m esset divisibilis per quadratum, tum factor quadratus per divisionem tolli posset. Ponatur porro m esse numerum tam ad a quam b primum, erunt ob $ma^4-m^3b^4=m(aa-mbb)(aa+mbb)$ toti factores inter se primi, ideoque singuli esse deberent quadrata. Facto ergo $m=pp$, deberet $(aa-ppbb)(aa+ppbb)$ esse quadratum, quod fieri nequit. Simili modo ob $2ma^4-2m^3b^4=2m(aa-mbb)(aa+mbb)$, atque factores inter se vel primos vel binarium pro communi mensura habentes, erit vel $2m$ vel m quadratum: priori vero casu facto $2m=4pp$, oporteret esse $a^4-4p^4b^4$ quadratum, quod pariter fieri nequit. Sin autem $m=pp$, tum foret $2a^4-2p^4b^4$ quadratum, quod per theorema praecedens fieri nequit. At si m non fuerit primus respectu ipsius a, ponamus $m=rs$ atque $a=rc$, ubi notandum est r et s nu-

meros esse inter se primos, quia m nullum factorem quadratum habere ponitur. Quadrata ergo esse deberent istae formae $r^3sc^4 - r^3s^3b^4$ et $2r^3sc^4 - 2r^3s^3b^4$ seu $r^3sc^4 - rs^3b^4$ et $2r^3sc^4 - 2rs^3b^4$.

Ob factores autem harum formularum inter se primos, vel rs vel $2rs$ deberent esse quadrata, adeoque r et s vel $2s$ singulatim, unde formulae orirentur, quas quadrata esse non posse jam est ostensum. Q. E. D.

Coroll. 1. Hujusmodi igitur formae $mn(m^2a^4 - n^2b^4)$ et $2mn(m^2a^4 - n^2b^4)$ quadrata esse non possunt, quicunque etiam numeri loco m, n, a et b accipiantur.

Coroll. 2. Si igitur $maa + nbb$ fuerit quadratum, nec $m^2naa - mn^2bb$ nec $2m^2naa - 2mn^2bb$ quadrata esse poterunt. Atque si $maa - nbb$ fuerit quadratum, nec $m^2naa + mn^2bb$ nec $2m^2naa + 2mn^2bb$ quadrata esse poterunt.

Coroll. 3. Ponamus $maa + nbb = cc$; erit $m = \frac{cc - nbb}{aa}$, quadratum ergo esse neque $n(cc - nbb)(cc - 2nbb)$ neque $2n(cc - nbb)(cc - 2nbb)$ poterit. Atque si fuerit $m = \frac{cc + nbb}{aa}$, tum neutra istarum formularum $n(cc + nbb)(cc + 2nbb)$ et $2n(cc + nbb)(cc + 2nbb)$ poterit esse quadratum.

Coroll. 4. Si ponatur $c = \pm pp + nqq$ et $b = 2pq$, sequentes obtinebuntur formulae $n(p^6 \pm 6nppqq + n^2q^4)$ et $2n(p^6 \pm 6nppqq + n^2q^4)$, quae nullo modo quadrata effici poterunt.

Theorema 6. Neque $ma^4 + m^3b^4$ neque $2ma^4 + 2m^3b^4$ potest esse quadratum.

Demonstratio. Dico primo, si fuerit $mp^2 \mp mq^2$ quadratum, tum nec $mp^2 + mq^2$ nec $2mp^2 + 2mq^2$ quadratum ullo modo esse posse: fieret enim vel $m^2(p^4 - q^4)$ vel $2m^2(p^4 - q^4)$ quadratum contra jam demonstrata. Faciamus autem $mp^2 - mq^2$ quadratum ponendo radicem ejus $= \frac{(p-q)a}{b}$, erit $mp + mq = \frac{a^2p - a^2q}{bb}$, unde reperitur $q = \frac{p(aa - mbb)}{aa + mbb}$. Sit igitur $p = a^2 + mb^2$, erit $q = a^2 - mb^2$ adeoque $p^2 + q^2 = 2a^4 + 2m^2b^4$. Quadratum ergo esse non poterit primo $mp^2 + mq^2 = 2ma^4 + 2m^3b^4$; deinde $2mp^2 + 2mq^2 = 4ma^4 + 4m^3b^4$. Ex his colligitur neque $ma^4 + m^3b^4$ neque $2ma^4 + 2m^3b^4$ quadratum esse posse. Q. E. D.

Coroll. In his igitur duobus theorematibus evictum est, nullos numeros in istis formis $ma^4 \pm m^3b^4$ et $2ma^4 \pm 2m^3b^4$ posse esse quadratos. In his autem formulis praecedentes omnes continentur.

Theorema 7. *Fermatianum.* Nullus numerus trigonalis in integris potest esse biquadratum praeter unitatem.

Demonstratio. Omnis numerus trigonalis hac forma $\frac{x(x+1)}{2}$ continetur. Demonstrandum ergo hanc formulam $\frac{x(x+1)}{2}$ nunquam esse posse biquadratum, siquidem loco x numeri integri substituantur, excepto casu $x = 1$. Notandum autem est vel x esse numerum parem vel imparem; priori igitur casu $\frac{x}{2}(x+1)$, posteriori vero $x\frac{(x+1)}{2}$ esse debere biquadratum; in quorum factorum utroque bini factores sunt inter se primi, ideoque uterque esse deberet biquadratum. Sit igitur priori casu $\frac{x}{2} = m^4$, seu $x = 2m^4$, debebitque $x + 1 = 2m^4 + 1$ esse biquadratum. Posteriori vero casu sit $\frac{x+1}{2} = m^4$, ut sit $x = 2m^4 - 1$, quod itidem oportet sit biquadratum. Hanc ob rem

biquadratum esse deberet $2m^4 \pm 1$. Ponatur $2m^4 \pm 1 = n^4$, erit $4m^4 = 2n^4 \mp 2$; deberet ergo $2n^4 \mp 2$ esse $4m^4$, hoc est quadratum. Supra autem demonstratum est $2a^4 \pm 2b^4$, adeoque etiam $2n^4 \pm 2$ nunquam quadratum esse posse, praeter casum $n = 1$. Posito autem $n = 1$, fit m vel $= 0$ vel $= 1$; atque x vel $= 0$ vel $= 1$. Nullus igitur numerus integer datur, qui loco x substitutus redderet $\frac{x(x+1)}{2}$ biquadratum, praeter casus $x = 0$ et $x = 1$. Quamobrem in integris nullus exstat numerus trigonalis, qui esset biquadratus praeter unitatem et cyphram. Q. E. D.

Coroll. 1. Si ponatur $\frac{xx+x}{2} = y^4$, erit $4xx + 4x + 1 = 8y^4 + 1 = (2x+1)^2$. Ex quo sequitur, numeris integris loco y substituendis, hanc formam $8y^4 + 1$ nunquam esse posse quadratum, praeter casus $y = 0$ et $y = 1$.

Coroll. 2. Si ponatur $8y^4 + 1 = z^2$, fiet $16y^4 = 2z^2 - 2$. Quocirca $2z^2 - 2$ nunquam esse potest biquadratum, quicunque numerus integer loco z substituatur, praeter casus $z = 1$ et $z = 3$.

Theorema 8. Summa trium biquadratorum, quorum duo sunt aequalia inter se, seu istiusmodi forma $a^4 + 2b^4$, quadratum esse nequit, nisi sit $b = 0$.

Demonstratio. Ponamus $a^4 + 2b^4$ esse quadratum, ejusque radicem $a^2 + \frac{m}{n} b^2$; ubi tam a et b quam m et n numeri erunt inter se primi. Facta autem aequatione erit $2n^2b^2 = 2mna^2 + m^2b^2$, atque $\frac{b^2}{a^2} = \frac{2mn}{2n^2 - m^2}$; quae fractio vel simplicissimam jam habet formam, vel divisione per 2 ad simplicissimam erit reducibilis. Ponamus primo $2mn$ et $2n^2 - m^2$ numeros esse inter se primos, quod evenit, si m sit numerus impar; eritque $b^2 = 2mn$ et $a^2 = 2n^2 - m^2$; hic duo evolvendi sunt casus, quorum alter est si n est numerus impar, alter si n est par; illo casu, quo n est impar, manifestum est ob m etiam imparem, $2mn$ fieri non posse quadratum; hoc vero casu, quo n est numerus par, fieri nequit $a^2 = 2n^2 - m^2$ seu $a^2 + m^2 = 2n^2$, ob a et m numeros impares, et $2n^2$ numerum pariter parem. Habeant igitur $2mn$ et $2n^2 - m^2$ communem divisorem 2, quod accidit si m sit numerus par, puta $m = 2k$, eritque n numerus impar; habebitur ergo $\frac{b^2}{a^2} = \frac{4kn}{2nn - 4kk} = \frac{2kn}{nn - 2kk}$, ubi $2kn$ et $nn - 2kk$ numeri erunt inter se primi. Hinc igitur ob b^2 et a^2 pariter inter se primos, erit $b^2 = 2kn$ et $a^2 = nn - 2kk$. At hic $2kn$ fieri nequit quadratum, nisi sit k numerus par. Sit ergo k numerus par, atque tam n quam $2k$ debebunt esse quadrata; fiat igitur $n = cc$ et $2k = 4dd$, ubi erit c numerus impar, hocque facto habebitur $a^2 = c^4 - 8d^4$. Quo igitur investigemus an $c^4 - 8d^4$ possit esse quadratum, ponamus ejus radicem esse $cc - \frac{2p}{q} dd$, eritque $2q^2d^2 = pqc^2 - p^2d^2$; seu $\frac{dd}{cc} = \frac{pq}{pp + 2qq}$; ubi iterum tam c et d quam p et q sunt numeri inter se primi. Hic denuo duo casus sunt notandi, sive p sit numerus impar sive par. Sit ergo primo p numerus impar; habebitur ob pq et $pp + 2qq$ numeros inter se primos, $dd = pq$ et $cc = pp + 2qq$; necesse ergo est ut tam p quam q sit quadratum; quamobrem pono $p = x^2$ et $q = y^2$, prodibitque $cc = x^4 + 2y^4$; quare si $a^4 + 2b^4$ esset quadratum, tum quoque foret $x^4 + 2y^4$ quadratum, numerique x et y vehementer erunt minores quam a et b; ex iisque denuo minores inveniri possent, quod in integris fieri nequit. Pro secundo casu, quo p est numerus par, ponamus $p = 2r$, eritque $\frac{dd}{cc} = \frac{2qr}{4rr + 2qq} = \frac{qr}{2rr + qq}$; et ob q imparem, erunt qr et $2rr + qq$ numeri inter se primi. Erit ergo $dd = qr$ et $cc = 2rr + qq$, quare numerorum q et r uterque debet esse quadratus; positis itaque $q = xx$ et $r = yy$, fiet $cc = 2y^4 + x^4$; unde

patet, si $a^4 + 2b^4$ esset quadratum, tum quoque in numeris longe minoribus fore similem formam $x^4 + 2y^4$ quadratum. Quocirca $a^4 + 2b^4$ quadratum esse nequit, nisi sit $b = 0$. Q. E. D.

Coroll. 1. Quoniam invenimus $\frac{b^2}{a^2} = \frac{2mn}{2n^2 - m^2}$ posito $a^4 + 2b^4$ quadrato, sequitur $2mn(2n^2 - m^2)$ quadratum esse non posse; quicunque etiam numeri loco m et n substituantur.

Coroll. 2. Factis ergo $m = x^2$ et $n = y^2$, quadratum non erit haec forma $4y^4 - 2x^4$. Simili modo posito $2m = 4x^2$ et $n = y^2$, quadratum non erit haec forma $2y^4 - 4x^4$. Atque facto $m = x^2$ et $2n = 4y^2$, haec formula $8y^4 - x^4$ quadratum esse nequit.

Coroll. 3. Si generaliter fiat $m = \alpha x^2$ et $n = \beta y^2$, prodibit haec formula $2\alpha\beta(2\beta^2 y^4 - \alpha^2 x^4)$ seu $4\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$, quae nullo modo quadratum esse poterit.

Theorema 9. Si haec forma $a^4 + kb^4$ quadratum esse non potest, tum etiam haec forma $2k\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$ nullo pacto quadratum effici poterit.

Demonstratio. Ponamus formam propositam $a^4 + kb^4$ esse quadratum, ejusque radicem $= a^2 + \frac{m}{n} b^2$ erit $kn^2 b^2 = 2mna^2 + m^2 b^2$ atque $\frac{b^2}{a^2} = \frac{2mn}{kn^2 - m^2}$. Quia ergo $a^4 + kb^4$ quadratum esse nequit, tum etiam $\frac{2mn}{kn^2 - m^2}$ seu $2mn(kn^2 - m^2)$ quadratum esse non poterit. Fiat $m = \alpha x^2$ et $n = \beta y^2$, prodibit $2\alpha\beta(k\beta^2 y^4 - \alpha^2 x^4)$ seu $2k\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$, quae formula propterea quadratum esse non potest, quicunque numeri sive affirmativi sive negativi loco α et β substituantur. Q. E. D.

Coroll. 1. Fiat sive α sive β negativum, ut prodeat haec forma $2\alpha^3\beta x^4 - 2k\alpha\beta^3 y^4$, atque ponatur $2\alpha^3\beta = p^2$, erit $\beta = \frac{p^2}{2\alpha^3}$, unde illa forma transit in hanc $p^2 x^4 - \frac{kp^6}{4\alpha^8} y^4$. Quadratum ergo esse nequit haec formula $x^4 - 4ky^4$ posito $4y^4$ pro $\frac{p^4}{4\alpha^8} y^4$. Ex hac ergo formula ulterius sequitur hanc expressionem $2\alpha^3\beta x^4 + 8k\alpha\beta^3 y^4$ quadratum fieri non posse.

Coroll. 2. Ponatur in formula inventa $2k\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$, $2k\alpha\beta^3 = pp$, ut sit $\alpha = \frac{pp}{2k\beta^3}$: transibit illa in hanc $p^2 y^4 - \frac{p^6}{4k^3\beta^8} x^4$, ex qua sequitur $a^4 - 4kb^4$ quadratum esse non posse; unde ut ante $2\alpha^3\beta x^4 + 8k\alpha\beta^3 y^4$ quadratum esse non poterit.

Coroll. 3. Si ergo $a^4 + kb^4$ quadratum esse nequit, tum nec haec formula $2k\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$ nec haec $\alpha^3\beta x^4 + k\alpha\beta^3 y^4$ quadratum esse poterit, quae posterior ex corollariis praecedentibus sequitur scribendo 2α loco α.

Coroll. 4. Cum igitur $a^4 + b^4$ non possit esse quadratum, sequentes binae formulae

$$\alpha^3\beta x^4 + \alpha\beta^3 y^4 \quad \text{et} \quad 2\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$$

quadrata esse omnino non poterunt.

Coroll. 5. Atque quia $a^4 - b^4$ quadratum esse non potest, orientur hae duae novae formulae $\alpha^3\beta x^4 - \alpha\beta^3 y^4$ et $2\alpha^3\beta x^4 + 2\alpha\beta^3 y^4$, quae nullo modo quadrata reddi possunt.

Coroll. 6. Quoniam denique $a^4 + 2b^4$ quadratum esse nequit, istae quoque formulae

$$\alpha^3\beta x^4 + 2\alpha\beta^3 y^4 \quad \text{et} \quad 4\alpha\beta^3 y^4 - 2\alpha^3\beta x^4$$

non poterunt effici quadrata.

Scholion. Ex iis igitur, quae hactenus demonstravi, prodierunt sex sequentes formulae generaliores, quae nullo modo in quadrata transmutari possunt:

I. $\alpha^3\beta x^4 + \alpha\beta^3 y^4$	IV. $2\alpha^3\beta x^4 - 2\alpha\beta^3 y^4$
II. $\alpha^3\beta x^4 - \alpha\beta^3 y^4$	V. $2\alpha^3\beta x^4 + 2\alpha\beta^3 y^4$
III. $\alpha^3\beta x^4 + 2\alpha\beta^3 y^4$	VI. $2\alpha^3\beta x^4 - 4\alpha\beta^3 y^4$

Atque in his sex formulis omnes continentur, quas in praecedentibus formulis tractavimus. Ex his autem formulis possent, ut jam ante feci, formulae trinominales elici, quas aeque certum esset quadrata neutiquam reddi posse; sed iis exhibendis supersedeo, ad alia nonnulla theoremata progressurus, quae circa cubos versantur, atque ex istis formulis expediri nequeunt.

Theorema 10. Nullus cubus, ne quidem numeris fractis exceptis, unitate auctus quadratum efficere potest, praeter unicum casum, quo cubus est 8.

Demonstratio. Propositio ergo huc redit, ut $\frac{a^3}{b^3}+1$ nunquam esse possit quadratum, praeter casum quo $\frac{a}{b}=2$. Quocirca demonstrandum erit hanc formulam a^3b+b^4 nunquam fieri posse quadratum, nisi sit $a=2b$.

Haec autem expressio resolvitur in istos tres factores $b(a+b)(aa-ab+bb)$, qui primo quadratum constituere possunt, si esse posset $b(a+b)=aa-ab+bb$, unde prodit $a=2b$, qui erit casus, quem excepimus. Pono autem, ut ulterius pergam, $a+b=c$, seu $a=c-b$, qua facta substitutione habebitur $bc(cc-3bc+3bb)$, quam demonstrandum est quadratum esse non posse, nisi sit $c=3b$; sunt autem b et c numeri inter se primi. Hic autem duo occurrunt casus considerandi, prout c vel multiplum est ternarii vel secus: illo enim casu factores c et $cc-3bc+3bb$ communem divisorem habebunt 3, hoc vero omnes tres inter se erunt primi. Sit primo c non divisibile per 3, necesse erit, ut singuli illi tres factores sint quadrata, scilicet, b, et c, et $cc-3bc+3bb$ seorsim. Fiat ergo

$$cc-3bc+3bb=(\tfrac{m}{n}b-c)^2,\quad \text{erit}\quad \frac{b}{c}=\frac{3nn-2mn}{3nn-mm},\quad \text{vel}\quad \frac{b}{c}=\frac{2mn-3nn}{mm-3nn},$$

cujus fractionis termini erunt primi inter se, nisi m sit multiplum ternarii; sit ergo m per 3 non divisibile, erit vel $c=3nn-mm$, vel $c=mm-3nn$; et vel $b=3nn-2mn$, vel $b=2mn-3nn$. At cum $3nn-mm$ quadratum esse nequeat, ponatur $c=mm-3nn$, quod quadratum fiat radicis $m-\frac{p}{q}n$, hincque oritur

$$\frac{m}{n}=\frac{3qq+pp}{2pq},\quad \text{atque}\quad \frac{b}{nn}=\frac{2m}{n}-3=\frac{3qq-3pq+pp}{pq}.$$

Quadratum ergo esset haec formula $pq(3qq-3pq+pp)$, quae omnino similis est propositae $bc(3bb-3bc+cc)$ et ex multo minoribus numeris constat. At sit m multiplum ternarii, puta $m=3k$, erit

$$\frac{b}{c}=\frac{nn-2kn}{nn-3kk},$$

unde erit vel $c=nn-3kk$, vel $c=3kk-nn$; quia autem $3kk-nn$ quadratum esse nequit, ponatur $c=nn-3kk$, ejusque radix $n-\frac{p}{q}k$, unde fiet

$$\frac{n}{k}=\frac{3qq+pp}{2pq};\quad \text{seu}\quad \frac{k}{n}=\frac{2pq}{3qq+pp};\quad \text{atque}\quad \frac{b}{nn}=1-\frac{2k}{n}=\frac{pp+3qq-4pq}{3qq+pp}.$$

Quadratum ergo esse deberet $(pp + 3qq)(p - q)(p - 3q)$. Ponatur $p - q = t$ et $p - 3q = u$, erit $q = \frac{t-u}{2}$ et $p = \frac{3t-u}{2}$, illaque formula abit in hanc $tu(3tt - 3tu + uu)$, quae iterum similis est priori $bc(3bb - 3bc + cc)$. Restat ergo posterior casus, quo est c multiplum ternarii, puta $c = 3d$; atque quadratum esse debet $bd(bb - 3bd + 3dd)$, quae cum iterum similis sit priori, manifestum est utroque casu evenire non posse, ut formula proposita sit quadratum. Quamobrem praeter cubum 8, alius ne in fractis quidem datur, qui cum unitate faciat quadratum. Q. E. D.

Coroll. 1. Simili modo demonstrari potest nullum cubum unitate minutum esse posse quadratum; hocque ne quidem in fractis.

Coroll. 2. Hinc sequitur nec $x^6 + y^6$ nec $x^6 - y^6$ esse posse quadrata: atque nullum numerum trigonalem esse cubum praeter unitatem.



VI.

Theoremata circa divisores numerorum in hac forma $paa \pm qbb$ contentorum.

(Comment. XIV. 1744 — 46. p. 151.)

In sequentibus theorematibus litterae a et b designant numeros quoscunque integros, primos inter se, seu qui praeter unitatem nullum alium habeant divisorem communem.

Theorema 1. Numerorum in hac forma $aa + bb$ contentorum divisores primi omnes sunt vel 2, vel hujus formae $4m + 1$ numeri.

Theorema 2. Omnes numeri primi hujus formae $4m + 1$ vicissim in hac numerorum formula $aa + bb$ continentur.

Theorema 3. Summa ergo duorum quadratorum seu numerus hujus formae $aa + bb$ dividi nequit per ullum numerum hujus formae $4m - 1$.

Theorema 4. Numerorum in hac forma $aa + 2bb$ contentorum divisores primi omnes sunt vel 2, vel numeri in hac forma $8m + 1$, vel in hac $8m + 3$ contenti.

Theorema 5. Omnes numeri primi in hac $8m + 1$, vel hac $8m + 3$ forma contenti vicissim sunt numeri hujus formae $aa + 2bb$.

Theorema 6. Nullus numerus hujus formae $aa + 2bb$ dividi potest per ullum numerum hujus $8m - 1$, vel hujus $8m - 3$ formae.

Theorema 7. Numerorum in hac forma $aa + 3bb$ contentorum divisores primi omnes sunt vel 2, vel 3, vel in una harum formularum $12m + 1$, $12m + 7$ contenti.

Theorema 8. Omnes numeri primi in alterutra harum formularum $12m + 1$, vel $12m + 7$, sive in hac una $6m + 1$ contenti simul sunt numeri hujus formae $aa + 3bb$.

Theorema 9. Nullus numerus sive hujus $12m - 1$, sive hujus $12m - 7$ formae, hoc est nullus numerus hujus formae $6m - 1$ est divisor ullius numeri in hac forma $aa + 3bb$ contenti.

Theorema 10. Numerorum in hac forma $aa + 5bb$ contentorum divisores primi omnes sunt vel 2, vel 5, vel in una harum 4 formarum $20m + 1$, $20m + 3$, $20m + 7$, $20m + 9$ contenti.

Theorema 11. Si fuerint numeri $20m + 1$, $20m + 3$, $20m + 9$, $20m + 7$ primi, tum erit ut sequitur

$$20m + 1 = aa + 5bb;\quad 2(20m + 3) = aa + 5bb$$
$$20m + 9 = aa + 5bb;\quad 2(20m + 7) = aa + 5bb.$$

Theorema 12. Nullus numerus in una sequentium formularum contentus $20m - 1$, $20m - 3$, $20m - 9$, $20m - 7$ potest esse divisor ullius numeri hujus formae $aa + 5bb$.

Theorema 13. Numerorum in hac forma $aa + 7bb$ contentorum divisores primi omnes sunt vel 2, vel 7, vel in una sequentium sex formularum

		seu in una harum trium
$28m + 1$	$28m + 11$	$14m + 1$
$28m + 9$	$28m + 15$	$14m + 9$
$28m + 25$	$28m + 23$	$14m + 11$

sunt contenti.

Theorema 14. Si fuerint numeri in istis formulis $14m + 1$, $14m + 9$, $14m + 11$ contenti primi, tum simul in hac forma $aa + 7bb$ continentur.

Theorema 15. Nullus numerus hujus formae $aa + 7bb$ potest dividi per ullum numerum, qui in una sequentium sex formularum

		seu harum trium
$28m + 3$	$28m + 5$	$14m + 3$
$28m + 13$	$28m + 17$	$14m + 5$
$28m + 19$	$28m + 27$	$14m + 13$

contineatur.

Theorema 16. Numerorum in hac forma $aa + 11bb$ contentorum omnes divisores primi sunt vel 2, vel 11, vel continentur in una sequentium

10 formularum		seu 5 formularum
$44m + 1$	$44m + 3$	$22m + 1$
$44m + 9$	$44m + 27$	$22m + 3$
$44m + 37$	$44m + 23$	$22m + 9$
$44m + 25$	$44m + 31$	$22m + 5$
$44m + 5$	$44m + 15$	$22m + 15$

Theorema 17. Si fuerint numeri in his sive decem, sive quinque formulis contenti primi, tum simul erunt vel ipsi vel eorum quadrupli numeri hujus formae $aa + 11bb$.

Theorema 18. Nullus numerus hujus formae $aa + 11bb$ potest dividi per ullum numerum, qui contineatur in una sequentium

sive 10 formularum		sive 5 formularum
$44m + 7$	$44m + 29$	$22m + 7$
$44m + 13$	$44m + 35$	$22m + 13$
$44m + 17$	$44m + 39$	$22m + 17$
$44m + 19$	$44m + 41$	$22m + 19$
$44m + 21$	$44m + 43$	$22m + 21$

Theorema 19. Numerorum in hac forma $aa + 13bb$ contentorum omnes divisores primi sunt vel 2, vel 13, vel continentur in una sequentium 12 formularum:

$52m + 1$	$52m + 7$
$52m + 49$	$52m + 31$
$52m + 9$	$52m + 11$
$52m + 25$	$52m + 19$

$52m + 29$	$52m + 47$
$52m + 17$	$52m + 15$

Theorema 20. Omnes numeri primi, qui in priori formularum istarum columna continentur, simul sunt numeri hujus formae $aa + 13bb$. Numerorum autem primorum, qui in altera formularum columna continentur, dupla sunt numeri formae $aa + 13bb$.

Theorema 21. Nullus numerus hujus formae $aa + 13bb$ dividi potest per ullum numerum, qui contineatur in una sequentium formularum

$52m + 3$	$52m + 35$
$52m + 5$	$52m + 37$
$52m + 21$	$52m + 41$
$52m + 23$	$52m + 43$
$52m + 27$	$52m + 45$
$52m + 33$	$52m + 51$.

Theorema 22. Numerorum in hac forma $aa + 17bb$ contentorum omnes divisores primi sunt vel 2, vel 17, vel in una sequentium formularum continentur:

$68m + 1$	$68m + 3$
$68m + 9$	$68m + 27$
$68m + 13$	$68m + 39$
$68m + 49$	$68m + 11$
$68m + 33$	$68m + 31$
$68m + 25$	$68m + 7$
$68m + 21$	$68m + 63$
$68m + 53$	$68m + 23$.

Theorema 23. Omnes numeri primi, qui in priori harum formularum columna continentur, ad quos 2 referri debet, sunt formae $aa + 17bb$, vel ipsi quidem, vel eorum noncupla. Numerorum autem primorum in altera columna contentorum tripla sunt numeri formae $aa + 17bb$.

Theorema 24. Nullus numerus hujus formae $aa + 17bb$ dividi potest per ullum numerum, qui contineatur in aliqua sequentium formularum

$68m - 1$	$68m - 3$
$68m - 9$	$68m - 27$
$68m - 13$	$68m - 39$
$68m - 49$	$68m - 11$
$68m - 33$	$68m - 31$
$68m - 25$	$68m - 7$
$68m - 21$	$68m - 63$
$68m - 53$	$68m - 23$

Theorema 25. Numerorum in hac forma $aa + 19bb$ contentorum omnes divisores primi sunt vel 2, vel 19, vel continentur in una sequentium

18 formularum		vel harum 9
$76m+1$	$76m+5$	$38m+1$
$76m+25$	$76m+49$	$38m+5$
$76m+17$	$76m+9$	$38m+7$
$76m+45$	$76m+73$	$38m+9$
$76m+61$	$76m+7$	$38m+11$
$76m+35$	$76m+23$	$38m+17$
$76m+39$	$76m+43$	$38m+23$
$76m+63$	$76m+11$	$38m+25$
$76m+55$	$76m+47$	$38m+35$.

Theorema 26. Omnes numeri primi, qui in una harum formularum continentur, sunt vel ipsi, vel saltem quater sumti numeri hujus formae $aa+19bb$.

Theorema 27. Nullus numerus hujus formae $aa+19bb$ dividi potest per ullum numerum, qui contineatur in aliqua sequentium 9 formularum:

$38m-1$	$38m-9$	$38m-23$
$38m-5$	$38m-11$	$38m-25$
$38m-7$	$38m-17$	$38m-35$.

His igitur theorematibus continetur indoles formularum $aa+qbb$, si q fuerit numerus primus, ac primum quidem vidimus omnes divisores primos hujusmodi formularum esse vel 2, vel q, vel in talibus expressionibus $4qm+\alpha$ ita comprehendi posse, ut nullus divisor in iis non contineatur, tum vero, ut omnis numerus primus $4qm+\alpha$ simul sit divisor formulae cujusdam $aa+qbb$. Deinde etiam hoc colligere licet, si numerus primus formae $4qm+\alpha$ fuerit divisor cujusquam numeri $aa+qbb$, tum nullum numerum formae $4qm-\alpha$ divisorem esse posse ejusdem expressionis $aa+qbb$. Cum igitur inter formas divisorum formulae $aa+qbb$ semper contineatur haec $4mq+1$, manifestum est nullum numerum $aa+qbb$ dividi posse per ullum numerum formae $4mq-1$. Denique attendenti manifestum fiet, si q fuerit numerus primus formae $4n-1$, tum divisorum formas ad numerum duplo minorem redigi posse, ita ut ad formulas $2qm+\alpha$ revocari queant, quod fieri nequit, si q sit numerus primus formae $4n+1$. Si igitur pro hac forma $aa+(4n+1)bb$ divisor fuerit $4(4n+1)m+\alpha$, tum nullus numerus formae istius $4(4n+1)m+2(4n+1)+\alpha$ poterit esse divisor ejusdem expressionis $aa+(4n+1)bb$. Plures annotationes faciemus, cum etiam formulas $aa+qbb$, quando q non est numerus primus, fuerimus contemplati.

Theorema 28. Numerorum in hac forma $aa+6bb$, vel hac $2aa+3bb$ contentorum divisores primi omnes sunt vel 2, vel 3, vel in una sequentium formularum continentur

$24m+1$	$24m+7$
$24m+5$	$24m+11$.

Theorema 29. Omnes numeri primi formae vel $24m+1$, vel $24m+7$ continentur in expressione $aa+6bb$; at numeri primi istam formam $24m+5$ et $24m+11$ habentes continentur in expressione $3aa+2bb$.

Theorema 30. Nullus numerus sive $aa + 6bb$, sive $2aa + 3bb$ dividi potest per ullum numerum, qui contineatur in aliqua harum formularum

$24m - 1$	$24m - 5$
$24m - 7$	$24m - 11$.

Theorema 31. Numerorum in hac $aa + 10bb$, vel hac forma $2aa + 5bb$ contentorum divisores primi omnes sunt vel 2, vel 5, vel in una sequentium formularum continentur

$40m + 1$	$40m + 7$
$40m + 9$	$40m + 23$
$40m + 11$	$40m + 37$
$40m + 19$	$40m + 13$.

Theorema 32. Numeri primi in priori harum formularum columna contenti simul sunt numeri hujus formae $aa + 10bb$, et numeri primi in altera columna contenti sunt hujus formae $2aa + 5bb$.

Theorema 33. Nullus numerus sive hujus $aa + 10bb$, sive hujus $2aa + 5bb$ formae dividi potest per ullum numerum, qui in aliqua sequentium formularum contineatur

$40m - 1$	$40m - 7$
$40m - 9$	$40m - 23$
$40m - 11$	$40m - 37$
$40m - 19$	$40m - 13$.

Theorema 34. Numerorum in hac $aa + 14bb$, vel hac $2aa + 7bb$ forma contentorum divisores primi omnes sunt vel 2, vel 7, vel in una sequentium formularum continentur

$56m + 1$	$56m + 3$
$56m + 9$	$56m + 27$
$56m + 25$	$56m + 19$
$56m + 15$	$56m + 5$
$56m + 23$	$56m + 45$
$56m + 39$	$56m + 13$.

Theorema 35. Numeri primi in priori harum formularum columna contenti simul sunt numeri vel hujus $aa + 14bb$, vel $2aa + 7bb$ formae; qui autem in altera columna continentur, eorum tripla demum in altera istarum formularum comprehenduntur.

Theorema 36. Si in superioribus formulis signa + in — commutentur, tum nullus numerus in istis formulis contentus divisor erit vel formae $aa + 14bb$, vel $2aa + 7bb$.

Theorema 37. Numerorum in hac $aa + 15bb$, vel hac $3aa + 5bb$ forma contentorum divisores primi omnes sunt vel 2, vel 3, vel 5, vel in una sequentium formularum continentur

		vel harum 4
$60m + 31$	$60m + 1$	$30m + 1$
$60m + 17$	$60m + 47$	$30m + 17$
$60m + 19$	$60m + 49$	$30m + 19$
$60m + 23$	$60m + 53$	$30m + 23$.

Theorema 38. Numerorum in hac $aa + 21bb$, vel hac $3aa + 7bb$ forma contentorum divisores primi omnes sunt vel 2, vel 3, vel 7, vel in una sequentium formularum continentur:

$84m + 1$	$84m + 5$
$84m + 25$	$84m + 41$
$84m + 37$	$84m + 17$
$84m + 55$	$84m + 11$
$84m + 31$	$84m + 23$
$84m + 19$	$84m + 71$.

Theorema 39. Numerorum in hac $aa + 35bb$, vel hac $5aa + 7bb$ forma contentorum divisores primi omnes sunt vel 2, vel 5, vel 7, vel in una sequentium formularum continentur:

		vel harum
$140m + 1$	$140m + 3$	$70m + 1$
$140m + 9$	$140m + 27$	$70m + 3$
$140m + 81$	$140m + 103$	$70m + 9$
$140m + 29$	$140m + 87$	$70m + 11$
$140m + 121$	$140m + 83$	$70m + 13$
$140m + 109$	$140m + 47$	$70m + 17$
$140m + 11$	$140m + 33$	$70m + 27$
$140m + 99$	$140m + 17$	$70m + 29$
$140m + 51$	$140m + 13$	$70m + 33$
$140m + 39$	$140m + 117$	$70m + 39$
$140m + 71$	$140m + 73$	$70m + 47$
$140m + 79$	$140m + 97$	$70m + 51$.

Theorema 40. Numerorum in aliqua harum formularum contentorum

$$aa + 30bb; \quad 2aa + 15bb$$
$$3aa + 10bb; \quad 5aa + 6bb$$

divisores primi omnes sunt vel 2, vel 3, vel 5, vel in una sequentium formularum continentur:

$120m + 1$	$120m + 11$
$120m + 13$	$120m + 23$
$120m + 49$	$120m + 59$
$120m + 37$	$120m + 47$
$120m + 17$	$120m + 67$
$120m + 101$	$120m + 31$
$120m + 113$	$120m + 43$
$120m + 29$	$120m + 79$.

Theoremata haec sufficiunt ad sequentes annotationes formandas, ex quibus natura divisorum hujusmodi formularum $paa + qbb$ penitius perspicietur.

Annotatio 1. Formula $paa + qbb$ nullum habet divisorem, quin sit simul divisor formulae $aa + pqbb$. Cujus quidem rei ratio facile patet; nam qui numerus est divisor formulae $paa + qbb$,

idem dividet hanc formam $ppaa + pqbb$, hoc est hanc $aa + pqbb$, posito a loco pa. Hanc ob rem sufficiet istam unicam formam $aa + Nbb$ considerasse, quippe quae ratione divisorum hanc $paa + qbb$ in se complectitur.

Annotatio 2. Inter numeros primos, qui ullum numerum in hac formula $aa + Nbb$ contentum dividunt, primum occurrit binarius. Si enim N sit numerus impar, sumendis pro a et b numeris imparibus, formula $aa + Nbb$ fiet per 2 divisibilis; at si N sit numerus par, sumto a pari, formula quoque per 2 fit divisibilis. Deinde vero ipse numerus N vel quaelibet ejus pars aliquota poterit esse divisor formulae $aa + Nbb$, quod sumendo $a = N$ est perspicuum.

Annotatio 3. Reliqui divisores primi omnes formulae $aa + Nbb$ in istiusmodi expressionibus $4Nm + \alpha$ comprehendi possunt ita, ut etiam vicissim omnes numeri primi in formis istis $4Nm + \alpha$ contenti simul sint divisores formulae $aa + Nbb$. Praeterea si expressio $4Nm + \alpha$ praebeat divisores formulae $aa + Nbb$, tum nullus numerus hujusmodi $4Nm - \alpha$ poterit esse divisor ullius numeri in formula $aa + Nbb$ contenti.

Annotatio 4. Habebit autem α certos quosdam valores, qui ab indole numeri N pendebunt; ac semper quidem unitas erit unus ex valoribus ipsius α. Tum vero, quia de numeris primis in formula $4Nm + \alpha$ contentis quaestio est, perspicuum est neque ullum numerum parem, neque ullum numerum, qui cum N communem habeat divisorem, valorem ipsius α constituere posse.

Annotatio 5. Valores autem ipsius α omnes erunt minores quam $4N$, si enim qui essent majores, per diminutionem numeri m minores quam $4N$ reddi possent. Hinc valores ipsius α erunt numeri impares minores quam $4N$, atque ad N primi. Neque vero omnes istiusmodi numeri impares ad N primi idoneos pro α valores exhibebunt, sed eorum semissis ab hoc officio excluditur, quoniam, si x fuerit valor ipsius α, tum $-x$ seu $4N - x$ ejus valor esse nequit; vicissimque si x non fuerit valor ipsius α, tum $4N - x$ certo ejus valor sit futurus.

Annotatio 6. Numerus igitur valorum ipsius α, ita ut $4Nm + \alpha$ contineat omnes divisores primos formulae $aa + Nbb$, sequenti modo definietur. Sint p, q, r, s, etc. numeri primi inter se diversi, excepto binario, qui seorsim est considerandus; atque

si fuerit	erit valorum ipsius α numerus
$N = 1$	1
$N = 2$	2
$N = p$	$p - 1$
$N = 2p$	$2(p - 1)$
$N = pq$	$(p - 1)(q - 1)$
$N = 2pq$	$2(p - 1)(q - 1)$
$N = pqr$	$(p - 1)(q - 1)(r - 1)$
$N = 2pqr$	$2(p - 1)(q - 1)(r - 1)$
etc.	

Annotatio 7. Quemadmodum autem unitas semper reperitur inter valores ipsius α, ita etiam quivis numerus quadratus impar et primus ad N locum habere debet in valoribus ipsius α. Posito

enim b numero pari $2c$, formula fiet $aa + 4Ncc$, quae, si sit numerus primus, contineri debet in expressione $4Nm + \alpha$. Ergo α erit aa, vel residuum, quod ex divisione ipsius aa per $4N$ remanet. Simili modo inter valores ipsius α reperiri debent omnes numeri $aa + N$, vel quae ex eorum per $4N$ divisione supererunt residua; posito enim $b = 2c + 1$, fiet $aa + Nbb = aa + N + 4N(cc + c)$, qui, si fuerit numerus primus, debebit $aa + N$ esse valor ipsius α.

Annotatio 8. Intelligitur etiam, si x fuerit valor ipsius α, tum quoque xx (quod quidem ex praecedente patet) et omnes omnino potestates ipsius x, puta x^μ, inter valores ipsius α locum habere debere. Deinde, si praeter x quoque y fuerit valor ipsius α, tum quoque xy et generaliter $x^\mu y^\nu$ dabit quoque valorem ipsius α. Scilicet si $x^\mu y^\nu$ majus fuerit quam $4N$, per hoc dividatur, et residuum erit valor ipsius α. Simili modo, si insuper z fuerit valor ipsius α, tum etiam $x^\mu y^\nu z^\lambda$ erit valor ipsius α. Hincque ex cognito uno vel aliquot valoribus ipsius α facili negotio omnes omnino ejus valores inveniuntur.

Annotatio 9. Sit x quicunque numerus primus ad $4N$, eoque minor, atque vel $+x$, vel $-x$ valor erit ipsius α. Si igitur fuerit x numerus primus, ex sequenti tabula intelligetur, quibus casibus $+x$, quibusque $-x$ valorem ipsius α praebeat:

Si	erit
$N = 3n - 1$	$\alpha = +3$
$N = 3n + 1$	$\alpha = -3$
$N = \begin{cases} 5n+1 \\ 5n+4 \end{cases}$	$\alpha = +5$
$N = \begin{cases} 5n+2 \\ 5n+3 \end{cases}$	$\alpha = -5$
$N = \begin{cases} 7n+3 \\ 7n+5 \\ 7n+6 \end{cases}$	$\alpha = +7$
$N = \begin{cases} 7n+1 \\ 7n+2 \\ 7n+4 \end{cases}$	$\alpha = -7$
$N = \begin{cases} 11n+2 \\ 11n+6 \\ 11n+7 \\ 11n+8 \\ 11n+10 \end{cases}$	$\alpha = +11$
$N = \begin{cases} 11n+1 \\ 11n+3 \\ 11n+4 \\ 11n+5 \\ 11n+9 \end{cases}$	$\alpha = -11$

Si propositus sit numerus quicunque primus, qui utrum signo $+$ an $-$ affectus valorem ipsius α praebeat, ita investigabitur. Bini casus debent evolvi, alter, quo propositus numerus primus est formae $4u + 1$, alter quo est formae $4u - 1$. Priori casu erit $\alpha = +(4u + 1)$, si fuerit $N = (4u + 1)n + tt$, at $\alpha = -(4u + 1)$, si fuerit $N \neq (4u + 1)n + tt$. Posteriori casu autem erit $\alpha = +(4u - 1)$, si sit $N \neq (4u - 1)n + tt$, at $\alpha = -(4u - 1)$, si $N = (4u - 1)n + tt$. Ubi notandum est, quemadmodum signum $=$ aequalitatem denotat, ita signum $\neq$ aequalitatis impossibilitatem designare. Quod si autem fuerit pro utroque casu $N = (4u \pm 1)n + s$, erit quoque $N = (4u \pm 1)n + s^\nu$, denotante ν numerum quemcunque integrum, unde ista tabella pro quibusvis numeris primis sine negotio construitur.

Annotatio 10. Quoniam inter formas divisorum primorum ipsius $aa + Nbb$ habetur $4Nm + 1$, eadem expressio $aa + Nbb$ per nullum numerum dividi poterit, qui contineatur in hac forma $4Nm - 1$. Simili modo cum $4Nm + tt$ exhibeat formam divisorum expressionis $aa + Nbb$, sequitur nullum numerum hujusmodi $4Nm - tt$ posse esse divisorem ullius numeri in hac forma $aa + Nbb$ contenti, si quidem, quod semper pono, a et b sint numeri inter se primi. Hanc ob rem impossibilis erit ista aequatio $(4Nm - tt)u = aa + Nbb$, ideoque erit $4Nmu - ttu - Nbb = aa$, si quidem fuerint $4Nmu - ttu$ et Nbb numeri inter se primi, quod cum certo eveniat, si $b = 1$ et $t = 1$, nanciscimur istud

Consectarium. Nullus numerus hac formula $4abc - b - c$ contentus unquam esse potest quadratus.

Annotatio 11. Si fuerit N numerus hujus formae $4n - 1$, tum formae divisorum ad numerum duplo minorem rediguntur, ita ut in formulis hujusmodi $2Nm + \alpha$ comprehendantur. Scilicet si fuerit $4Nm + \alpha$ divisorum forma, tum quoque $4Nm + 2N + \alpha$ erit forma divisorum. Quare cum $2Nm + tt$ sit forma divisorum, sequitur nullum numerum $2Nm - tt$ divisorem esse posse formae $aa + Nbb$. Hinc erit $(2Nm - tt)u = aa + Nbb$, existente $N = 4n - 1$, unde oritur hoc

Consectarium. Nullus numerus hujus formae $2abc - b - c$, si vel b vel c fuerit numerus impar $4n - 1$, unquam potest esse quadratus.

Annotatio 12. Si fuerit N numerus impar hujusmodi $4n + 1$, vel etiam numerus impariter par, tum divisorum formae ad numerum duplo minorem redigi non possunt. Scilicet si $4Nm + \alpha$ fuerit divisor formae $aa + Nbb$, tum $4Nm + 2N + \alpha$ ejusdem formae divisor esse non poterit. Hinc $2(2m + 1)N + tt$ non erit divisor formae $aa - Nbb$, ideoque haec aequatio

$$(2(2m + 1)N + tt)u = aa + Nbb$$

erit aequatio impossibilis, si quidem sint a et b numeri primi inter se, et N sit vel numerus impar formae $4n + 1$, vel numerus impariter par. Ex quo sequitur istud

Consectarium. Nullus numerus hujus formae $2abc - b + c$, existente a numero impari, et b vel impariter pari vel impari formae $4n + 1$, unquam esse potest quadratus.

Scholion 1. Quae hic sunt allata sufficienter declarant indolem divisorum hujusmodi formularum $aa + Nbb$, simulque inserviunt ad omnes divisorum formas expedite inveniendas, quibus cognitis quoque eae numerorum formae innotescunt, quae nunquam praebere queant divisores formulae $aa + Nbb$. Cum igitur haec pateant ad omnes valores ipsius N, sive sint numeri primi, sive compositi, reliquum est, ut etiam casus evolvamus, quibus N denotet numeros negativos tam primos quam compositos; perspicuum autem est formulam $paa - qbb$ nullum divisorem habere posse, quin sit divisor hujus $aa - pqbb$ seu $pqaa - bb$, unde sufficiet hujusmodi tantum formas $aa - Nbb$ evolvisse.

Theorema 41. Numerorum in hac forma $aa - bb$ contentorum divisores primi omnes sunt vel 2, vel $4m \pm 1$; nullus scilicet datur numerus, qui non sit divisor differentiae duorum quadratorum. Vicissim autem omnes numeri, praeter impariter pares, ipsi sunt differentiae duorum quadratorum.

Theorema 42. Numerorum in hac forma $aa - 2bb$ contentorum omnes divisores primi sunt vel 2, vel hujus formae $8m \pm 1$. Omnesque numeri primi hujus formae $8m \pm 1$ ipsi infinitis modis in formula $aa - 2bb$ continentur.

Theorema 43. Numerorum in hac forma contentorum $aa - 3bb$ omnes divisores primi sunt vel 2, vel 3, vel hujus formae $12m \pm 1$. Atque vicissim omnes hujusmodi numeri primi simul in hac $aa - 3bb$, vel hac $3aa - bb$ forma infinitis modis continentur.

Theorema 44. Omnes divisores primi hujus formae $aa - 5bb$ sunt vel 2, vel 5, vel continentur

in altera harum formularum	vel in hac una
$20m \pm 1$, $20m \pm 9$	$10m \pm 1$.

Omnesque numeri primi in his formis contenti simul sunt divisores formae $aa - 5bb$.

Theorema 45. Omnes divisores primi hujus formae $aa - 7bb$ sunt vel 2, vel 7, vel in una sequentium formularum continentur

$$28m \pm 1; \quad 28m \pm 3; \quad 28m \pm 9;$$

atque vicissim omnes numeri primi in his formis contenti simul sunt divisores formae $aa - 7bb$.

Theorema 46. Omnes divisores primi hujus formae $aa - 11bb$ sunt vel 2, vel 11, vel in una sequentium formarum continentur

$$44m \pm 1; \quad 44m \pm 5; \quad 44m \pm 7; \quad 44m \pm 9; \quad 44m \pm 19;$$

atque vicissim omnes numeri primi in his formulis contenti simul sunt divisores formae $aa - 11bb$, quae reciprocatio in omnibus sequentibus theorematibus locum habet.

Theorema 47. Omnes divisores primi formae $aa - 13bb$ sunt vel 2, vel 13, vel in sequentibus formulis continentur:

		quae revocantur ad has
$52m \pm 1$	$52m \pm 3$	$26m \pm 1$
$52m \pm 9$	$52m \pm 25$	$26m \pm 3$
$52m \pm 23$	$52m \pm 17$	$26m \pm 9$.

Theorema 48. Omnes divisores primi numerorum hujus formae $aa - 17bb$ sunt vel 2, vel 17, vel in sequentibus formulis continentur:

		quae revocantur ad has
$68m \pm 1$	$68m \pm 9$	$34m \pm 1$
$68m \pm 13$	$68m \pm 19$	$34m \pm 9$
$68m \pm 33$	$68m \pm 25$	$34m \pm 13$
$68m \pm 21$	$68m \pm 15$	$34m \pm 15$.

Theorema 49. Omnes divisores primi numerorum hujus formae $aa - 19bb$ sunt vel 2, vel 19, vel in sequentibus formulis continentur

$76m \pm 1$	$76m \pm 3$	$76m \pm 9$
$76m \pm 27$	$76m \pm 5$	$76m \pm 15$
$76m \pm 31$	$76m \pm 17$	$76m \pm 25$.

Theorema 50. Omnes divisores primi numerorum formae hujus $aa - 6bb$ sunt vel 2, vel 3, vel in his formulis continentur:

$$24m \pm 1 \qquad 24m \pm 5.$$

Theorema 51. Omnes divisores primi numerorum formae $aa - 10bb$ sunt vel 2, vel 5, vel in his formulis continentur:

$$40m \pm 1 \qquad 40m \pm 3$$
$$40m \pm 9 \qquad 40m \pm 13.$$

Theorema 52. Omnes divisores primi numerorum hujus formae $aa - 14bb$ sunt vel 2, vel 7, vel in his formulis continentur:

$$56m \pm 1 \qquad 56m \pm 5 \qquad 56m \pm 25$$
$$56m \pm 13 \qquad 56m \pm 9 \qquad 56m \pm 11.$$

Theorema 53. Omnes divisores primi numerorum hujus formae $aa - 22bb$ sunt vel 2, vel 11, vel in his formulis continentur:

$$88m \pm 1 \qquad 88m \pm 3 \qquad 88m \pm 9$$
$$88m \pm 27 \qquad 88m \pm 7 \qquad 88m \pm 21$$
$$88m \pm 25 \qquad 88m \pm 13 \qquad 88m \pm 39$$
$$88m \pm 29.$$

Theorema 54. Omnes divisores primi numerorum hujus formae $aa - 15bb$ sunt vel 2, vel 3, vel 5, vel in his formulis continentur:

$$60m \pm 1 \qquad 60m \pm 7 \qquad 60m \pm 11 \qquad 60m \pm 17.$$

Theorema 55. Omnes divisores primi numerorum hujus formae $aa - 21bb$ sunt vel 2, vel 3, vel 7, vel in his formis continentur:

		quae revocantur ad has
$84m \pm 1$	$84m \pm 5$	$42m \pm 1$
$84m \pm 25$	$84m \pm 41$	$42m \pm 5$
$84m \pm 37$	$84m \pm 17$	$42m \pm 17.$

Theorema 56. Omnes divisores primi numerorum hujus formae $aa - 33bb$ sunt vel 2, vel 3, vel 11, vel in his formulis continentur:

		quae revocantur ad has
$132m \pm 1$	$132m \pm 17$	$66m \pm 1$
$132m \pm 25$	$132m \pm 29$	$66m \pm 17$
$132m \pm 35$	$132m \pm 65$	$66m \pm 25$
$132m \pm 49$	$132m \pm 41$	$66m \pm 29$
$132m \pm 37$	$132m \pm 31$	$66m \pm 31.$

Theorema 57. Omnes divisores primi numerorum hujus formae $aa - 35bb$ sunt vel 2, vel 5, vel 7, vel in his formulis continentur:

$$140m \pm 1 \qquad 140m \pm 9 \qquad 140m \pm 59$$
$$140m \pm 29 \qquad 140m \pm 19 \qquad 140m \pm 31$$
$$140m \pm 13 \qquad 140m \pm 23 \qquad 140m \pm 67$$
$$140m \pm 43 \qquad 140m \pm 33 \qquad 140m \pm 17.$$

Theorema 58. Omnes divisores primi numerorum hujus formae $aa - 30bb$ sunt vel 2, vel 3, vel 5, vel in his formulis continentur:

$120m \pm 1$	$120m \pm 13$	$120m \pm 49$
$120m \pm 37$	$120m \pm 7$	$120m \pm 29$
$120m \pm 17$	$120m \pm 19.$	

Theorema 59. Omnes divisores primi numerorum hujus formae $aa - 105bb$ sunt vel 2, vel 3, vel 5, vel 7, vel continentur in his formulis.:

		quae revocantur ad has
$420m \pm 1$	$420m \pm 13$	$210m \pm 1$
$420m \pm 169$	$420m \pm 97$	$210m \pm 13$
$420m \pm 23$	$420m \pm 121$	$210m \pm 23$
$420m \pm 107$	$420m \pm 131$	$210m \pm 41$
$420m \pm 109$	$420m \pm 157$	$210m \pm 53$
$420m \pm 59$	$420m \pm 73$	$210m \pm 59$
$420m \pm 101$	$420m \pm 53$	$210m \pm 73$
$420m \pm 151$	$420m \pm 137$	$210m \pm 79$
$420m \pm 89$	$420m \pm 103$	$210m \pm 89$
$420m \pm 79$	$420m \pm 187$	$210m \pm 97$
$420m \pm 41$	$420m \pm 113$	$210m \pm 101$
$420m \pm 209$	$420m \pm 197$	$210m \pm 103.$

Annotatio 13. Numerorum ergo in formula $aa - Nbb$ contentorum divisores primi omnes sunt vel 2, vel divisores numeri N, vel in ejusmodi formulis $4Nm \pm \alpha$ comprehenduntur. Quodsi enim $4Nm + \alpha$ fuerit forma divisorum, tum quoque $4Nm - \alpha$ erit divisorum forma: secus atque in formulis $aa + Nbb$, quarum si $4Nm + \alpha$ fuerit divisor, tum $4Nm - \alpha$ nullum unquam praebere potest divisorem ejusdem formulae.

Annotatio 14. Posita ergo $4Nm \pm \alpha$ pro forma divisorum generali numerorum in hac expressione $aa - Nbb$ contentorum, littera α plerumque plures significabit numeros, inter quos unitas semper continetur; tum vero quia hic de divisoribus primis sermo est, inter valores ipsius α nullus erit numerus par nec ullus divisor numeri N. Deinde etiam manifestum est, omnes valores ipsius α ita ordinari posse, ut sint minores quam $2N$. Si enim sit $4Nm + 2N + b$ divisor, tum posito $m - 1$ loco m, divisor erit $4Nm - (2N - b)$. Erunt ergo valores ipsius α numeri impares primi ad N, minores quam $2N$, horumque numerorum omnium imparium et primorum ad N et minorum quam $2N$, semissis tantum praebebit idoneos valores ipsius α; reliqui exhibebunt formulas, in quibus plane nullus continetur divisor. Perpetuo scilicet totidem habebuntur formulae divisorum, quot sunt contrariae, solo excepto casu, quo $N = 1$.

Annotatio 15. Quod ad numerum valorum ipsius α pro formula divisorum $4Nm \pm \alpha$ attinet, quoniam ob signum ambiguum quaevis formula est duplex, hic quoque eadem valebit regula, quam supra annot. 6 dedi. Sic in ultimo theoremate, quo erat $N = 105 = 3.5.7$, numerus valorum ipsius α erit $= 2.4.6 = 48$, seu cum quaevis formula sit gemina, numerus formularum fit 24, quot etiam exhibuimus.

Annotatio 16. Sicut autem unitas perpetuo inter valores ipsius α reperitur, ita etiam quivis numerus quadratus, qui sit primus ad $4N$, valorem idoneum pro α suppeditabit. Posito enim $b = 2c$, formula $aa - Nbb$ abit in $aa - 4Ncc$, seu $4Ncc - aa$, ex quo patet quemvis numerum quadratum aa, qui sit primus ad $4N$, exhibere valorem idoneum pro α, sumendo scilicet residuo, quod in divisione ipsius aa per $4N$ remanet. Simili modo ponendo $b = 2c + 1$, formula $Nbb - aa$ abit in $4N(cc + c) + N - aa$, unde etiam omnes numeri $N - aa$, seu $aa - N$, qui quidem sint primi ad $4N$, idoneos valores pro α praebebunt. Deinde quoque notandum est, si sint x, y, z, valores ipsius α, tum quoque x^{μ}, y^{ν}, z^{ζ} itemque omnia producta, quae ex numeris x, y, z eorumve potestatibus quibuscunque resultant, valores ipsius α esse exhibitura; unde cognito uno vel aliquot valoribus ipsius α facili negotio omnes reperiuntur.

Annotatio 17. Quo autem clarius appareat, cujusmodi valores littera α perpetuo sit habitura, tabulam sequentem adjicere visum est, similem ejus, quae annot. 9 habetur.

Erit scilicet	si fuerit	
$\alpha = 3$	$N = 3n + 1$	
$\alpha \neq 3$	$N = 3n - 1$	
$\alpha = 5$	$N = 5n$	$+1, -1$
$\alpha \neq 5$	$N = 5n$	$+2, -2$
$\alpha = 7$	$N = 7n$	$+1, +2, -3$
$\alpha \neq 7$	$N = 7n$	$-1, -2, +3$
$\alpha = 11$	$N = 11n$	$+1, -2, +3, +4, +5$
$\alpha \neq 11$	$N = 11n$	$-1, +2, -3, -4, -5$
$\alpha = 13$	$N = 13n$	$+1, -1, +3, -3, +4, -4$
$\alpha \neq 13$	$N = 13n$	$+2, -2, +5, -5, +6, -6$

Annotatio 18. Ex hac igitur tabula numeri primi, qui idoneos valores pro α praebeant, facile dignosci, simulque inepti rejici possunt. Proposito scilicet numero primo p, omnes numeri quadrati in hujusmodi formulis $pn + \vartheta$ comprehendi possunt, quae prodeunt ponendo pro ϑ numeros quadratos, seu residua, quae ex divisione quadratorum per p remanent. Quare si N fuerit hujusmodi numerus $pn + tt$, tum inter formas divisorum $4Nm \pm \alpha$ formulae $aa - Nbb$, seu $Nbb - aa$, habe-

bitur $\alpha = p$; sin autem numerus N non contineatur in forma $pn + tt$, tum nullus numerus in formula hac $4Nm \pm p$ contentus poterit esse divisor ullius numeri hujus formae $aa - Nbb$.

Annotatio 19. Si fuerit N numerus impar formae $4n + 1$, tum expressionis $aa - Nbb$ divisorum formae $4Nm \pm \alpha$ ad duplo pauciores reduci possunt, ita ut exhiberi possint hoc modo: $2Nm \pm \alpha$. Hoc scilicet casu, si $4Nm \pm \alpha$ fuerit forma divisorum, tum quoque $4Nm \pm (2N - \alpha)$ erit divisorum forma; sic cum casu $N = 13$, una divisorum formulae $aa - 13bb$ forma esset $52m \pm 3$, erit quoque $52m \pm 23$ forma divisorum.

Annotatio 20. Sin autem fuerit N vel numerus impariter par, vel numerus impar formae $4n - 1$, tum ista formarum dividentium reductio ad duplo pauciores non succedit. Scilicet si hoc casu formulae $aa - Nbb$ fuerit $4Nm \pm \alpha$ divisorum forma, tum $4Nm \pm (2N - \alpha)$ talis non erit, hoc est: nullus numerus in forma $2(2m \pm 1)N \pm \alpha$ contentus erit divisor ullius numeri hujusmodi $aa - Nbb$. Posito ergo $\alpha = tt$, erit $(2(2m \pm 1)N \pm tt)u = aa - Nbb$. Unde consequimur sequens

Consectarium. Nullus numerus in hac forma $2abc \pm c + b$ contentus unquam potest esse quadratus, si quidem fuerit a numerus impar, et b numerus seu impariter par, seu impar hujus formae $4n - 1$.

Scholion 2. Hujusmodi formulae magis speciales, quae nunquam quadrata fieri queant, innumerabiles superioribus deduci possunt. Consideremus enim priorum formam $aa + Nbb$, sitque $4Nm + A$ ejusmodi formula, ut nullus numerus in ea contentus possit esse divisor formae $aa + Nbb$. Erit ergo $aa + Nbb = (4Nm + A)u$, denotante hoc signo $=$ aequationem impossibilem, ex quo oritur $aa = 4Nmu + Au - Nbb$. Sit $b = Ac$, fiet $aa = 4Nmu + Au - NAAcc$. Ponatur porro $u = NAcc + d$, eritque $aa = 4NNAmcc + 4Nmd + Ad$. Sit $d = 4NNn$, erit

$$aa = 16N^3mn + 4NNAmcc + 4NNAn.$$

Dividatur haec formula per quadratum $4NN$ ac ponatur $c = 1$, eritque $4Nmn + Am + An$ formula, quae nunquam poterit esse quadratum, si quidem forma $aa + Nbb$ non possit dividi per ullum numerum in hac formula $4Nm + A$ contentum. Ex superioribus ergo theorematibus colligimus nullum numerum, qui in una sequentium expressionum contineatur, fieri posse quadratum:

$4mn - (m+n)$	$4mn + 3(m+n)$
$8mn - (m+n)$	$8mn + 7(m+n)$
$8mn - 3(m+n)$	$8mn + 5(m+n)$
$12mn - (m+n)$	$12mn + 11(m+n)$
$12mn - 7(m+n)$	$12mn + 5(m+n)$
$20mn - (m+n)$	$20mn + 19(m+n)$
$20mn - 3(m+n)$	$20mn + 17(m+n)$
$20mn - 7(m+n)$	$20mn + 13(m+n)$
$20mn - 9(m+n)$	$20mn + 11(m+n)$
$24mn - (m+n)$	$24mn + 23(m+n)$
$24mn - 5(m+n)$	$24mn + 19(m+n)$
$24mn - 7(m+n)$	$24mn + 17(m+n)$
$24mn - 11(m+n)$	$24mn + 13(m+n)$

$28mn - (m+n)$	$28mn + 27(m+n)$
$28mn - 9(m+n)$	$28mn + 19(m+n)$
$28mn - 11(m+n)$	$28mn + 17(m+n)$
$28mn - 15(m+n)$	$28mn + 13(m+n)$
$28mn - 23(m+n)$	$28mn + 5(m+n)$
$28mn - 25(m+n)$	$28mn + 3(m+n)$

etc.

Notandum autem est in formulis alterius columnae numeros m et n respectu coefficientis ipsius $m+n$ primos esse oportere. Hanc restrictionem requirit ea conditio, quam initio stabilivimus, ut in forma $aa+Nbb$ numeri a et b sint inter se numeri primi: nisi enim haec conditio observetur, quilibet numerus posset esse divisor istius formae. Ceterum hac conditione observata ex praecedentibus perspicuum est, si $4Nmn - A(m+n)$ quadratum esse nequeat, tum quoque hanc latius patentem $4Nmn - A(m+n) \pm 4Np(m+n)$ quadratum esse non posse.

Scholion 3. Contemplemur jam expressionem $aa - Nbb$, cujus nullus divisor contineatur in formula hac $4Nm \pm A$. Erit ergo $aa - Nbb = 4Nmu \pm Au$, seu $aa = 4Nmu + NAA \pm Au$. Ponatur $NA \pm u = d$, seu $u = \pm d \mp NA$, eritque $aa = \pm 4Nmd \mp 4NNAm + Ad$; sit $d = \pm 4NNn$, fietque $16N^3mn \mp 4NNAm \pm 4NNAn = aa$, unde patet nullum numerum contentum in hac formula $4Nmn \pm A(m-n)$ quadratum esse posse. Neque ergo etiam ullus numerus in hac expressione $4Nmn \pm A(m-n) \pm 4Np(m-n)$ contentus quadratum esse poterit, si modo conditio ante memorata observetur, ut a et b sint numeri inter se primi. Hinc itaque ex theorematibus posterioribus deducuntur sequentes formulae, quae nunquam numeros quadratos praebere possunt:

$8mn \pm 3(m-n)$	$8mn \pm 5(m-n)$
$12mn \pm 5(m-n)$	$12mn \pm 7(m-n)$
$20mn \pm 3(m-n)$	$20mn \pm 17(m-n)$
$20mn \pm 7(m-n)$	$20mn \pm 13(m-n)$
$24mn \pm 7(m-n)$	$24mn \pm 17(m-n)$
$24mn \pm 11(m-n)$	$24mn \pm 13(m-n)$
$28mn \pm 5(m-n)$	$28mn \pm 23(m-n)$
$28mn \pm 11(m-n)$	$28mn \pm 17(m-n)$
$28mn \pm 13(m-n)$	$28mn \pm 15(m-n)$

etc.

attendenti autem facile patebit ambos numeros m et n respectu coefficientis ipsius $(m-n)$ primos esse debere: alioquin enim, si verbi gratia in formula $12mn \pm 5(m-n)$ poneretur $m = 5p$ et $n = 5q$, prodiret $12.25pq \pm 25(p-q)$, neque adeo haec formula $12pq \pm (p-q)$ quadratum esse posset, quod tamen est falsum.

VII.

Theoremata circa divisores numerorum.

(N. Comment. I. 1747 — 48. p. 20. Exhib. 1748 Oct. 17.)

Quovis tempore summi geometrae agnoverunt in natura numerorum plurimas praeclarissimas proprietates esse absconditas, quarum cognitio fines matheseos non mediocriter esset amplificatura. Primo quidem intuitu doctrina numerorum ad arithmeticae elementa referenda videtur, atque vix quicquam in ea inesse putatur, quod ullam sagacitatem aut vim analyseos requirat. Qui autem diligentius in hoc genere sunt versati, non solum veritates demonstratu difficillimas detexerunt, sed etiam ejusmodi, quarum certitudo percipiatur, etiamsi demonstrari nequeat. Plurima hujusmodi theoremata sunt prolata ab insigni geometra Fermatio, quorum veritas, quamvis demonstratio lateat, non minus evicta videtur. Atque hoc imprimis omnem attentionem meretur, in mathesi adeo pura ejusmodi dari veritates, quos nobis cognoscere liceat, cum tamen eas demonstrare non valeamus; atque hoc adeo in arithmetica usu venit, quae tamen prae reliquis matheseos partibus maxime pertractata ac perspecta haberi solet: neque facile affirmare ausim, an similes veritates in reliquis partibus reperiantur. In geometria certe nulla occurrit propositio, cujus vel veritas vel falsitas firmissimis rationibus evinci nequeat. Cum igitur quaevis veritas eo magis abstrusa censeatur, quo minus ad ejus demonstrationem aditus pateat, in arithmetica certe, ubi natura numerorum perpenditur, omnium abstrusissimas contineri negare non poterimus. Non desunt quidem inter summos mathematicos viri, qui hujusmodi veritates prorsus steriles, ideoque non dignas indicant, in quarum investigatione ulla opera collocetur; at praeterquam quod cognitio omnis veritatis per se sit excellens, etiamsi ab usu populari abhorrere videatur, omnes veritates, quas nobis cognoscere licet, tantopere inter se connexae deprehenduntur, ut nulla sine temeritate tanquam prorsus inutilis repudiari possit. Deinde etsi quaepiam propositio ita comparata videatur, ut sive vera sit sive falsa, nihil inde ad nostram utilitatem redundet, tamen ipsa methodus, qua ejus veritas vel falsitas evincitur, plerumque nobis viam ad alias utiliores veritates cognoscendas patefacere solet. Hanc ob rem non inutiliter me operam ac studium in indagatione demonstrationum quarundam propositionum impendisse confido, quibus insignes circa divisores numerorum proprietates continentur. Neque vero haec de divisoribus doctrina omni caret usu, sed nonnunquam in analysi non contemnendam praestat utilitatem. Imprimis vero non dubito, quin methodus ratiocinandi, qua sum usus, in aliis gravioribus investigationibus aliquando non parum subsidii afferre possit. Propositiones autem, quas hic demonstratas exhibeo, respiciunt divisores numerorum in hac formula $a^n \pm b^n$ contentorum, quarum nonnullae jam ab ante memorato Fermatio, sed sine demonstratione, sunt publicatae. Quoniam igitur hic perpetuo de numeris integris sermo instituetur, omnes alphabeti litterae hic constanter numeros integros indicabunt.

1. **Theorema 1.** Si p fuerit numerus primus, omnis numerus contentus in hac forma $(a+b)^p - a^p - b^p$ divisibilis erit per p.

Demonstratio. Si binomium $(a+b)^p$ modo consueto evolvatur, erit

$$(a+b)^p = a^p + \frac{p}{1}a^{p-1}b + \frac{p(p-1)}{1.2}a^{p-2}b^2 + \frac{p(p-1)(p-2)}{1.2.3}a^{p-3}b^3 + \ldots$$
$$+ \frac{p(p-1)(p-2)}{1.2.3}a^3b^{p-3} + \frac{p(p-1)}{1.2}a^2b^{p-2} + \frac{p}{1}ab^{p-1} + b^p,$$

qua expressione substituta, binisque terminis, qui easdem habent uncias, conjunctis, erit

$$(a+b)^p - a^p - b^p = \frac{p}{1}ab(a^{p-2} + b^{p-2}) + \frac{p(p-1)}{1.2}a^2b^2(a^{p-4} + b^{p-4})$$
$$+ \frac{p(p-1)(p-2)}{1.2.3}a^3b^3(a^{p-6} + b^{p-6})$$
$$+ \frac{p(p-1)(p-2)(p-3)}{1.2.3.4}a^4b^4(a^{p-8} + b^{p-8}) + \text{etc.}$$

Hic primo notandum est omnes uncias, quamquam sub forma fractionum apparent, nihilominus esse numeros integros, cum exhibeant, uti constat, numeros figuratos. Quaelibet ergo uncia cum factorem habeat p, divisibilis erit per p, nisi is alicubi per factorem denominatoris vel prorsus tollatur, vel dividatur. At ubique omnes factores denominatorum minores sunt quam p, quia adeo non ultra $\frac{1}{2}p$ crescunt, ideoque factor numeratorum p nusquam per divisionem tollitur. Deinde cum p sit per hypoth. numerus primus, is nusquam per divisionem minuetur. Quocirca singulae unciae

$$\frac{p}{1}; \quad \frac{p(p-1)}{1.2}; \quad \frac{p(p-1)(p-2)}{1.2.3}; \quad \text{etc.}$$

hincque tota expressio $(a+b)^p - a^p - b^p$ perpetuo per numerum p, siquidem fuerit numerus primus, erit divisibilis. Q. E. D.

2. **Coroll. 1.** Si ergo ponatur $a = 1$ et $b = 1$, erit $2^p - 2$ semper divisibilis per p, si quidem fuerit p numerus primus. Cum igitur sit $2^p - 2 = 2(2^{p-1} - 1)$, alterum horum factorum per p divisibilem esse oportet. At nisi sit $p = 2$, prior factor 2 per p non est divisibilis, unde sequitur formam $2^{p-1} - 1$ perpetuo per p esse divisibilem, si p fuerit numerus primus praeter binarium.

3. **Coroll. 2.** Ponendis ergo pro p successive numeris primis, erit $2^2 - 1$ divisibile per 3; $2^4 - 1$ per 5; $2^6 - 1$ per 7; $2^{10} - 1$ per 11 etc. quod in minoribus numeris per se fit perspicuum, in maximis autem aeque erit certum. Sic cum 641 sit numerus primus, iste numerus $2^{640} - 1$ necessario per 641 erit divisibilis. Seu si potestas 2^{640} per 641 dividatur, post divisionem supererit residuum $= 1$.

4. **Theorema 2.** Si utraque harum formularum $a^p - a$ et $b^p - b$ fuerit divisibilis per numerum primum p, tum quoque ista formula $(a+b)^p - a - b$ divisibilis erit per eundem numerum primum p.

Demonstratio. Cum per § 1 $(a+b)^p - a^p - b^p$ sit divisibilis per numerum p, si fuerit primus, atque hic formulae $a^p - a$ et $b^p - b$ per p divisibiles assumantur, erit quoque summa istarum trium formularum nempe $(a+b)^p - a - b$ per p, si fuerit numerus primus, divisibilis. Q. E. D.

5. **Coroll. 1.** Si ponatur $b = 1$, cum $1^p - 1 = 0$ sit divisibile per p; sequitur, si formula $a^p - a$ fuerit divisibilis per p, tum quoque formulam $(a + 1)^p - a - 1$ fore per p divisibilem.

6. **Coroll. 2.** Cum igitur assumta formula $a^p - a$ per p divisibili, sit quoque formula $(a + 1)^p - a - 1$ per p divisibilis: simili modo in eadem hypothesi erit haec quoque formula $(a + 2)^p - a - 2$, hincque porro haec $(a + 3)^p - a - 3$, etc. atque generaliter haec $c^p - c$ divisibilis per p.

7. **Theorema 3.** Si p fuerit numerus primus, omnis numerus hujus formae $c^p - c$ per p erit divisibilis.

Demonstratio. Si in § 6 ponatur $a = 1$, cum sit $a^p - a = 0$ per p divisibilis, sequitur has quoque formulas $2^p - 2$; $3^p - 3$; $4^p - 4$; etc. et generatim hanc $c^p - c$ fore per numerum primum p divisibilem. Q. E. D.

8. **Coroll. 1.** Quicunque ergo numerus integer pro c assumatur, denotante p numerum primum, omnes numeri in hac forma $c^p - c$ contenti erunt divisibiles per p.

9. **Coroll. 2.** Cum autem sit $c^p - c = c\,(c^{p-1} - 1)$, vel ipse numerus c vel $c^{p-1} - 1$ divisibilis erit per p, utrumque autem simul per p divisibilem esse non posse manifestum est. Quare si numerus c non fuerit divisibilis per p, haec forma $c^{p-1} - 1$ certe per p erit divisibilis.

10. **Coroll. 3.** Si ergo p fuerit numerus primus, omnes numeri in hac forma contenti $a^{p-1} - 1$ erunt divisibiles per p, exceptis iis casibus, quibus ipse numerus a per p est divisibilis.

11. **Theorema 4.** Si neuter numerorum a et b divisibilis fuerit per numerum p, tum omnis numerus hujus formae $a^{p-1} - b^{p-1}$ erit divisibilis per p.

Demonstratio. Cum neque a neque b sit divisibilis per p, atque p denotet numerum primum, tam haec forma $a^{p-1} - 1$, quam haec $b^{p-1} - 1$ erit divisibilis per p. Hinc ergo quoque differentia istarum formularum $a^{p-1} - b^{p-1}$ erit divisibilis per p. Q. E. D.

12. **Coroll. 1.** Cum omnis numerus primus praeter binarium, cujus ratio dividendi per se est manifesta sit impar, ponatur $2m + 1$ pro p, atque perspicuum erit, omnes numeros in hac forma $a^{2m} - b^{2m}$ contentos esse divisibiles per $p = 2m + 1$, siquidem neque a neque b seorsim fuerit per $2m + 1$ divisibilis.

13. **Coroll. 2.** Quia b non est divisibilis per $2m + 1$, etiam b^{2m} et $2b^{2m}$ non divisibile erit per $2m + 1$. Quare si $2b^{2m}$ addatur ad formulam $a^{2m} - b^{2m}$, quae est divisibilis per $2m + 1$, prodibit formula $a^{2m} + b^{2m}$, quae per $2m + 1$ non erit divisibilis, nisi uterque numerus a et b seorsim per $2m + 1$ sit divisibilis.

14. **Coroll. 3.** Quoniam ob $2m$ numerum parem formula $a^{2m} - b^{2m}$ factores habet

$$(a^m - b^m)\,(a^m + b^m),$$

necesse est ut horum factorum alter sit divisibilis per $2m + 1$; ambo autem simul per numerum $2m + 1$ divisibiles esse nequeunt. Quare si $2m + 1$ fuerit numerus primus, et neque a neque b divisibile sit per $2m + 1$, tum vel $a^m - b^m$, vel $a^m + b^m$ erit divisibile per $2m + 1$.

15. **Coroll. 4.** Si m sit numerus par, puta $= 2n$, atque $a^m - b^m$ seu $a^{2n} - b^{2n}$ divisibilis per $2m + 1 = 4n + 1$, tum ob eandem rationem vel $a^n - b^n$, vel $a^n + b^n$ divisibile erit per numerum primum $4n + 1$.

16. **Theorema 5.** Summa duorum quadratorum $aa + bb$ per nullum numerum primum hujus formae $4n - 1$ unquam dividi potest, nisi utriusque radix seorsim a et b sit divisibilis per $4n - 1$.

Demonstratio. Si $4n - 1$ fuerit numerus primus, neque a et b per illum sint divisibiles, tum $a^{4n-2} - b^{4n-2}$ erit divisibile per $4n-1$ (v. § 11), hincque ista formula $a^{4n-2} + b^{4n-2}$ non erit divisibilis per $4n - 1$, neque propterea ullus ejus factor. At cum $4n - 2 = 2(2n - 1)$ sit numerus impariter par, formula $a^{4n-2} + b^{4n-2}$ factorem habet $aa + bb$, quare fieri nequit, ut iste factor $aa + bb$, hoc est ulla duorum quadratorum summa sit divisibilis per $4n - 1$. Q. E. D.

17. **Coroll. 1.** Cum omnes numeri primi vel ad hanc formam $4n + 1$, vel ad hanc $4n - 1$ revocentur, si $4n - 1$ non fuerit numerus primus, divisorem habebit formae $4n - 1$; namque ex meris numeris formae $4n + 1$ nunquam numerus formae $4n - 1$ resultare potest. Quare cum summa duorum quadratorum per nullum numerum primum formae $4n - 1$ dividi possit, per nullum quoque numerum ejusdem formae $4n - 1$, etiamsi non sit primus, dividi poterit.

18. **Coroll. 2.** Summa ergo duorum quadratorum $aa + bb$ per nullum numerum hujus seriei:

3, 7, 11, 15, 19, 23, 27, 31, 35, etc.

est divisibilis. Omnes ergo numeri primi praeter binarium, qui unquam divisores esse possunt summae duorum quadratorum, continentur in hac forma $4n + 1$; siquidem numeri a et b inter se communem divisorem non habeant.

19. **Coroll. 3.** Cum omnis numerus sit vel primus, vel productum ex primis, summa duorum quadratorum nullum numerum primum pro divisore habebit, nisi qui contineatur in hac forma $4n + 1$. Divisores ergo primi summae duorum quadratorum continebuntur in hac serie:

2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc.

20. **Scholion.** Quod numerus hujus formae $4n - 1$ nunquam possit esse summa duorum quadratorum, facile intelligitur. Numeri enim quadrati vel sunt pares vel impares, illi in hac forma $4a$, hi vero in hac $4b + 1$ continentur. Quare ut summa duorum quadratorum sit numerus impar, alterum par alterum impar esse oportet; hinc oritur forma $4a + 4b + 1$, seu $4n + 1$, ideoque nullus numerus hujus formae $4n - 1$ summa duorum quadratorum esse potest. Quod vero summa duorum quadratorum ne divisorem quidem formae $4n - 1$ admittat, ab omnibus scriptoribus methodi Diophanteae semper est affirmatum: nemo autem unquam, quantum mihi constat, id demonstravit, excepto Fermatio, qui autem suam demonstrationem nunquam publicavit, ita ut mihi quidem videar primus hanc veritatem publice demonstrasse: nullum numerum vel hujus formae $4n - 1$, vel per numerum ejusdem formae divisibilem unquam esse posse summam duorum quadratorum. Hinc ergo sequitur omnem summam duorum quadratorum inter se primorum vel esse numerum primum, vel binario excepto alios divisores non habere nisi qui in forma $4n + 1$ contineantur.

21. **Theorema 6.** Omnes divisores summae duorum biquadratorum inter se primorum sunt vel 2, vel numeri hujus formae $8n + 1$.

Demonstratio. Sint a^4 et b^4 duo biquadrata inter se prima, erit vel utrumque impar, vel alterum par et alterum impar; priori casu summae $a^4 + b^4$ divisor erit 2; utroque vero casu divisores impares, si qui fuerint, in hac forma $4n + 1$ continebuntur. Cum enim biquadrata simul

sint quadrata, nullus divisor formae $4n-1$ locum invenit (16). At numeri $4n+1$ vel ad hanc formam $8n+1$, vel ad hanc $8n-3$ revocantur. Dico autem nullum numerum formae $8n-3$ esse posse divisorem summae duorum biquadratorum. Ad hoc demonstrandum sit primo $8n-3$ numerus primus, atque per eum divisibilis erit haec forma $a^{8n-4}-b^{8n-4}$, unde haec forma $a^{8n-4}+b^{8n-4}$ per numerum $8n-3$ prorsus non erit divisibilis, nisi uterque numerus a et b seorsim divisionem admittat, qui casus autem assumtione, quod ambo numeri a et b sint inter se primi, excluditur. Cum igitur forma $a^{8n-4}+b^{8n-4}=a^{4(2n-1)}+b^{4(2n-1)}$ dividi nequeat per $8n-3$, nullus quoque ejus factor per $8n-3$ dividi poterit. At ob $2n-1$ numerum imparem, illius formae factor erit a^4+b^4, qui ergo per nullum numerum primum formae $8n-3$ dividi potest. Hinc omnes numeri primi praeter binarium, qui unquam formam a^4+b^4 divident, erunt hujusmodi $8n+1$. Ex multiplicatione autem duorum pluriumve talium divisorum nunquam numerus formae $8n-3$ oritur: ex quo sequitur nullum prorsus numerum hujus formae $8n-3$, sive sit primus sive compositus, summam duorum biquadratorum inter se primorum dividere. Q. E. D.

22. **Coroll. 1.** Cum omnes numeri impares in una harum quatuor formarum contineantur: $8n\pm1$ et $8n\pm3$, praeter numeros in forma prima $8n+1$ contentos nullus alius poterit esse divisor summae duorum biquadratorum.

23. **Coroll. 2.** Omnes ergo divisores primi summae duorum biquadratorum inter se primorum erunt vel 2, vel in hac serie contenti: 17, 41, 73, 89, 97, 113, 137, 193, etc. quae complectitur omnes numeros primos formae $8n+1$.

24. **Coroll. 3.** Si quis ergo numerus, puta N, fuerit summa duorum biquadratorum, tum is vel erit primus, vel alios non habebit divisores, nisi qui in forma $8n+1$ contineantur; unde investigatio divisorum mirum in modum contrahitur.

25. **Coroll. 4.** Nullus igitur numerus, qui divisorem habet non in forma $8n+1$ contentum, erit summa duorum biquadratorum, nisi forte habeat quatuor divisores aequales, qui autem in consideratione biquadratorum rejici solent.

26. **Theorema 7.** Omnes divisores hujusmodi numerorum a^8+b^8 si quidem a et b sunt numeri inter se primi, sunt vel 2, vel in hac forma $16n+1$ continentur.

Demonstratio. Quia a^8 et b^8 simul sunt biquadrata, eorum summa a^8+b^8 alios non admittet divisores, nisi qui in forma $8n+1$ contineantur. At numeri in hac forma $8n+1$ contenti sunt vel $16n+1$, vel $16n-7$. Sit $16n-7$ numerus primus, ac per eum dividi non poterit forma $a^{16n-8}+b^{16n-8}$ (13), seu $a^{8(2n-1)}+b^{8(2n-1)}$, neque propterea ullus ejus factor. Verum ob $2n-1$ numerum imparem, haec forma divisorem habet a^8+b^8, quae ergo per nullum numerum primum $16n-7$ erit divisibilis, ac propterea alios divisores primos habere nequit, nisi qui in forma $16n+1$ contineantur. Ex multiplicatione autem duorum pluriumve hujusmodi numerorum $16n+1$, perpetuo productum ejusdem formae nascitur, neque unquam numerus formae $16n-7$ resultare potest. Unde cum nullus numerus formae $16n-7$ divisor ipsius a^8+b^8 existere possit, necesse est, ut omnes hujus formae a^8+b^8 divisores, si quos habet, sive sint primi sive compositi, perpetuo in hac formula $16n+1$ contineantur. Q. E. D.

27. **Coroll. 1.** Nullus igitur numerus, qui in hac forma $16n+1$ non includitur, unquam esse potest divisor summae duarum potestatum octavi gradus inter se primarum.

28. **Coroll. 2.** Si quis ergo voluerit numeri cujuspiam hujus formae a^8+b^8 divisores investigare, is divisionem per nullos alios numeros primos nisi in hac forma $16n+1$ contentos, tentet, cum demonstratum sit omnes reliquos numeros primos hujus formae divisores esse non posse.

29. **Theorema 8.** Summa duarum hujusmodi potestatum $a^{2^m}+b^{2^m}$, quarum exponens est dignitas binarii, alios divisores non admittit, nisi qui contineantur in hac forma $2^{m+1}n+1$.

Demonstratio. Quemadmodum demonstravimus omnes divisores formae a^2+b^2 in hac forma $4n+1$ contineri, hincque ulterius divisores omnes formae a^4+b^4 in $8n+1$, et formae a^8+b^8 in $16n+1$ contineri evicimus; ita simili modo ostendi potest formam $a^{16}+b^{16}$ nullos alios divisores admittere nisi in formula $32n+1$ contentos. Dehinc porro intelligemus formas $a^{32}+b^{32}$, $a^{64}+b^{64}$ etc. alios divisores habere non posse nisi qui in formulis $64n+1$, $128n+1$ etc. includantur. Sicque in genere patebit formae $a^{2^m}+b^{2^m}$ alios non dari divisores, nisi qui in formula $2^{m+1}n+1$ contineantur. Q. E. D.

30. **Coroll. 1.** Nullus ergo numerus primus, qui in hac forma $2^{m+1}n+1$ non includitur, unquam esse potest divisor ullius numeri in hac forma $a^{2^m}+b^{2^m}$ contenti.

31. **Coroll. 2.** Divisores ergo hujusmodi numeri $a^{2^m}+b^{2^m}$ inquisiturus inutiliter operam suam consumeret, si aliis numeris primis praeter eos, quos forma $2^{m+1}n+1$ suppeditat, divisionem tentare vellet.

32. **Scholion 1.** Fermatius affirmaverat, etiamsi id se demonstrare non posse ingenue esset confessus, omnes numeros ex hac forma $2^{2^m}+1$ ortos esse primos; hincque problema alias difficillimum, quo quaerebatur numerus primus dato numero major, resolvere est conatus. Ex ultimo theoremate autem perspicuum est, nisi numerus $2^{2^m}+1$ sit primus, eum alios divisores habere non posse praeter tales, qui in forma $2^{m+1}n+1$ contineantur. Cum igitur veritatem hujus effati Fermatiani pro casu $2^{32}+1$ examinare voluissem, ingens hinc compendium sum nactus, dum divisionem aliis numeris primis, praeter eos, quos formula $64n+1$ suppeditat, tentare non opus habebam. Huc igitur inquisitione reducta mox deprehendi ponendo $n=10$ numerum primum 641 esse divisorem numeri $2^{32}+1$, unde problema memoratum, quo numerus primus dato numero major requiritur, etiamnum manet insolutum.

33. **Scholion 2.** Summa duarum potestatum ejusdem gradus, uti a^m+b^m, semper habet divisores algebraice assignabiles, nisi m sit dignitas binarii. Nam si m sit numerus impar, tum a^m+b^m semper divisorem habet $a+b$, atque si p fuerit divisor ipsius m, tum quoque a^p+b^p formam a^m+b^m dividet. Sin autem m sit numerus par, in hac formula $2^n p$ continebitur, ita ut p sit numerus impar, hocque casu $a^{2^n}+b^{2^n}$ divisor erit formae a^m+b^m, existente $m=2^n p$. Atque si p habeat divisorem q, tum etiam $a^{2^n q}+b^{2^n q}$ erit divisor formae a^m+b^m. Quocirca a^m+b^m numerus primus esse nequit, nisi m sit dignitas binarii. Hoc igitur casu, si a^m+b^m non fuerit numerus primus, alios divisores habere nequit, nisi qui formula $2mn+1$ contineantur.

Contra autem, si differentia duarum potestatum ejusdem gradus proponatur $a^m - b^m$, ea semper divisorem habet $a - b$; praeterea vero si exponens m divisorem habeat p, erit quoque $a^p - b^p$ divisor formae $a^m - b^m$. Hinc si m sit numerus primus, forma $a^m - b^m$ praeter $a - b$ alium divisorem algebraice assignabilem non habebit; quare si $a^m - b^m$ fuerit numerus primus, necesse est ut m sit numerus primus et $a - b = 1$ Interim tamen ne his quidem casibus forma $a^m - b^m$ semper est numerus primus; sed quoties $2m + 1$ est numerus primus, per eum erit divisibilis. Praeterea vero etiam alios divisores habere potest, quos hic sum investigaturus.

34. **Theorema 9.** Si differentia potestatum $a^m - b^m$ fuerit divisibilis per numerum primum $2n + 1$, atque p sit maximus communis divisor numerorum m et $2n$, tum quoque $a^p - b^p$ erit divisibilis per $2n + 1$.

Demonstratio. Quia $2n + 1$ est numerus primus, erit $a^{2n} - b^{2n}$ divisibilis per $2n + 1$; et cum per hypothesin $a^m - b^m$ sit quoque divisibilis per $2n + 1$, sit $2n = \alpha m + q$, seu q sit residuum in divisione ipsius $2n$ per m remanens; et cum $a^{\alpha m} - b^{\alpha m}$ sit quoque per $2n + 1$ divisibilis, multiplicetur haec forma per a^q, erit $a^{\alpha m + q} - a^q b^{\alpha m}$ per $2n + 1$ divisibilis; at posito $\alpha m + q$ pro $2n$, est quoque $a^{\alpha m + q} - b^{\alpha m + q}$ per $2n + 1$ divisibilis: a qua formula si prior subtrahatur, residuum $a^q b^{\alpha m} - b^{\alpha m + q} = b^{\alpha m}(a^q - b^q)$ quoque per $2n + 1$ erit divisibile. Hinc cum b per hypothesin divisorem $2n + 1$ non habeat, necesse est ut $a^q - b^q$ per $2n + 1$ sit divisibile. Ponatur porro $m = \beta q + r$, et cum utraque haec formula $a^{\beta q + r} - b^{\beta q + r}$ et $a^{\beta q} - b^{\beta q}$ sit per $2n + 1$ divisibilis, multiplicetur posterior per a^r et a priori subtrahatur, atque residuum $b^{\beta q}(a^r - b^r)$, seu $a^r - b^r$ pariter per $2n + 1$ erit divisibile. Simili modo patebit, si fuerit $q = \gamma r + s$, tum formulam $a^s - b^s$ per $2n + 1$ fore divisibilem; atque si per hujusmodi continuam divisionem valores litterarum q, r, s, t, etc. investigentur, tandem pervenietur ad maximum communem divisorem numerorum m et $2n$, qui ergo si ponatur $= p$, erit $a^p - b^p$ divisibile per $2n + 1$. Q. E. D.

35. **Coroll. 1.** Si igitur m fuerit numerus ad $2n$ primus, maximus eorum communis divisor erit unitas, ac propterea si $a^m - b^m$ fuerit divisibile per numerum primum $2n + 1$, tum quoque $a - b$ per $2n + 1$ erit divisibile.

36. **Coroll. 2.** Si ergo differentia numerorum $a - b$ non fuerit divisibilis per $2n + 1$, tum quoque nulla hujusmodi forma $a^m - b^m$, ubi m est ad $2n$ numerus primus, per $2n + 1$ divisibilis esse potest.

37. **Coroll. 3.** Quodsi ergo m fuerit numerus primus, forma $a^m - b^m$ per numerum primum $2n + 1$ dividi non potest, nisi m sit divisor ipsius $2n$, posito quod $a - b$ non sit divisibile per $2n + 1$.

38. **Coroll. 4.** Existente ergo m numero primo, haec forma $a^m - b^m$ praeter divisorem $a - b$ alios divisores habere nequit, nisi qui includantur in hac formula $mn + 1$. Unde divisores numeri cujuspiam in hac forma $a^m - b^m$ contenti investigaturus divisionem tantum per numeros primos in forma $mn + 1$ contentos tentabit.

39. **Coroll. 5.** Nisi ergo numerus $2^m - 1$ sit primus, existente m numero primo, alios divisores habere non poterit, nisi qui includantur in hac forma $mn + 1$.

40. **Coroll. 6.** Si ergo m sit numerus primus, divisores formulae $a^m - b^m$, praeter $a - b$, si quidem a et b fuerint numeri inter se primi, continebuntur in hac serie:

$$2m + 1, \; 4m + 1, \; 6m + 1, \; 8m + 1, \; 10m + 1, \text{ etc.}$$

si hinc numeri non primi expungantur.

41. **Theorema 10.** Si formula $a^m \pm b^m$ divisorem habeat p, tum quoque haec expressio $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ per p erit divisibilis.

Demonstratio. Si potestates $(a \pm \alpha p)^m$ et $(b \pm \beta p)^m$ methodo consueta evolvantur, in utraque serie omnes termini praeter primum divisibiles erunt per p. Scilicet formula

$$(a \pm \alpha p)^m \pm (b \pm \beta p)^m$$

abibit in hac formam:

$$a^m \pm m a^{m-1} \alpha p + \frac{m(m-1)}{1 \cdot 2} a^{m-2} \alpha^2 p^2 \pm \text{ etc.}$$

$$\pm (b^m \pm m b^{m-1} \beta p + \frac{m(m-1)}{1 \cdot 2} b^{m-2} \beta^2 p^2 \pm \text{ etc.})$$

Unde perspicuum est si $a^m \pm b^m$ fuerit divisibile, tum quoque haec forma $(a \pm \alpha p)^m \pm (b \pm \beta p)^m$ per p erit divisibilis. Q. E. D.

42. **Coroll. 1.** Si igitur $a^m \pm 1$ fuerit divisibile per p, tum quoque haec formula $(a \pm \alpha p)^m \pm 1$ per p erit divisibilis.

43. **Coroll. 2.** Si $a^m \pm b^m$ fuerit divisibile per p, tum quoque haec formula $(a \pm \alpha p)^m \pm b^m$, vel haec $a^m \pm (b \pm \beta p)^m$ per p erit divisibilis.

44. **Scholion.** Eodem quoque modo generaliter demonstrari potest, si fuerit $Aa^m \pm Bb^m$ divisibilis per p, tum quoque hanc formam $A(a \pm \alpha p)^m \pm B(b \pm \beta p)^m$ fore per p divisibilem. Haecque veritas aeque locum invenit, sive p sit numerus primus sive secus. Quin etiam non opus est, ut utriusque potestatis idem sit exponens m, sed etiamsi essent inaequales, conclusio perinde valebit. Tum vero quoque si m fuerit numerus par, ex divisibilitate formulae $a^m \pm b^m$ per numerum p, divisibilitas etiam hujus formulae $(\alpha p \pm a)^m \pm (\beta p \pm b)^m$ sequitur. Verum haec aliaque similia ex algebrae elementis sponte patent.

45. **Theorema 11.** Si fuerit $a = ff \pm (2m + 1)\alpha$, et $2m + 1$ numerus primus, tum ista expressio $a^m - 1$ erit divisibilis per $2m + 1$.

Demonstratio. Cum sit $2m + 1$ numerus primus, per eum dividi poterit haec formula $f^{2m} - 1$, seu haec $(ff)^m - 1$. Hinc per theorema praecedens quoque ista formula

$$(ff \pm (2m - 1)\alpha)^m - 1$$

erit divisibilis per $2m + 1$. Quare si fuerit $a = ff \pm (2m + 1)\alpha$, formula $a^m - 1$ per numerum primum $2m + 1$ dividi poterit. Q. E. D.

46. **Coroll. 1.** Si ergo fuerit vel $a = (2m + 1)\alpha + 1$, vel $a = (2m + 1)\alpha + 4$, vel $a = (2m + 1)\alpha + 9$, vel $a = (2m + 1)\alpha + 16$, vel etc., tum formula $a^m - 1$ semper erit divisibilis per $2m + 1$, si quidem $2m + 1$ fuerit numerus primus.

47. **Coroll. 2.** Cum casus, quibus ipse numerus a est divisibilis per $2m + 1$, excludantur, manifestum est in formula $ff \pm (2m + 1)\alpha$ numerum f per $2m + 1$ divisibilem esse non posse. Hinc pro f omnes numeri assumi possunt, qui per $2m + 1$ non sint divisibiles.

48. **Coroll. 3.** Numeri ergo pro f assumendi sunt $(2m+1)k \pm 1$; $(2m+1)k \pm 2$; $(2m+1)k \pm 3$;........$(2m+1)k \pm m$: in his enim formulis omnes numeri per $2m+1$ non divisibiles continentur. Hinc sumendis quadratis formae ipsius a, si quidem partes per $2m+1$ divisibiles in unum colligantur, erunt sequentes:

$$(2m+1)p+1;\ (2m+1)p+4;\ (2m+1)p+9;\ldots\ldots\ldots(2m+1)p+mm,$$

quarum numerus est m.

49. **Coroll. 4.** Ad valores igitur ipsius a inveniendos, ut $a^m - 1$ per numerum primum $2m+1$ fiat divisibile, investigari oportet residua, quae in divisione cujusque numeri quadrati per $2m+1$ remanent. Si enim r fuerit hujus modi residuum, erit $(2m+1)p+r$ idoneus valor pro a.

50. **Coroll. 5.** Omnia haec residua r erunt autem minora quam $2m+1$, neque tamen omnes numeri minores quam $2m+1$ erunt valores ipsius r; quia numerus valorum ipsius r major esse nequit quam m. Dabuntur ergo semper m numeri, qui pro r adhiberi non poterunt.

51. **Coroll. 6.** Valores vero ipsius r erunt primo omnes numeri quadrati ipso $2m+1$ minores, tum vero residua, quae in divisione majorum quadratorum per $2m+1$ remanent, neque tamen unquam numerus omnium diversorum valorum ipsius r major esse poterit numero m.

52. **Scholion.** Ut usus hujus theorematis clarius appareat, atque per exempla numerica illustrari possit, sequentia problemata adjicere visum est, ex quibus non solum veritas theorematis luculentius perspicietur, sed etiam vicissim patebit, quoties a non habuerit valorem hic assignatum, toties formulam $a^m - 1$ non esse divisibilem per $2m+1$. Cum igitur haec formula $a^{2m} - 1$ semper sit divisibilis per $2m+1$, quoties $a^m - 1$ divisionem per $2m+1$ non admittit, toties $a^m + 1$ per $2m+1$ divisibile esse oportebit.

53. **Exempl. 1.** *Invenire valores ipsius* a, *ut* $a^2 - 1$ *fiat divisibile per* 5.

Residua, quae ex divisione quadratorum per 5 remanent sunt 1 et 4; hinc necesse est ut sit vel $a = 5p+1$, vel $a = 5p+4$, sive $a = 5p-1$. Priori casu fit $aa-1$, seu $(a-1)(a+1)$ $= 5p(5p+2)$, posteriori autem $= (5p-2)5p$; utroque ergo divisibilitas per 5 perspicitur. Sin autem fuerit vel $a = 5p+2$, vel $a = 5p+3$, neutro casu formula $aa-1$ per 5 erit divisibilis.

54. **Exempl. 2.** *Invenire valores ipsius* a, *ut haec forma* $a^3 - 1$ *fiat per* 7 *divisibilis.*

Tria residua, quae in divisione omnium quadratorum per 7 remanent, sunt 1, 2, 4. Hinc valores ipsius a sunt: $7p+1$, $7p+2$ et $7p+4$, sin autem fuerint vel $a = 7p+3$, vel $7p+5$, vel $7p+6$, tum non formula proposita $a^3 - 1$, sed haec $a^3 + 1$ per 7 fiet divisibilis.

55. **Exempl. 3.** *Invenire valores ipsius* a, *ut haec forma* $a^5 - 1$ *fiat per* 11 *divisibilis.*

Numeri quadrati per 11 divisi dabunt 5 diversa residua, quae sunt: 1, 3, 4, 5, 9. Hinc formula $a^5 - 1$ per 11 erit divisibilis, si fuerit $a = 11p+r$, denotante r unumquemque ex numeris 1, 3, 4, 5, 9. Sin autem pro a sumatur quidam ex his numeris 2, 6, 7, 8, 10 multiplo quocunque ipsius 11 auctus, tum $a^5 + 1$ per 11 erit divisibile.

56. **Theorema 12.** Si fuerit $a = f^3 \pm (3m+1)\alpha$, existente $3m+1$ numero primo, tum haec forma $a^m - 1$ semper erit per $3m+1$ divisibilis.

Demonstratio. Ob $3m+1$ numerum primum erit $f^{3m}-1$ divisibile per $3m+1$. At est $f^{3m}-1=(f^3)^m-1$, unde quoque haec formula $(f^3\pm(3m+1)\alpha)^m-1$ erit divisibilis per $3m+1$. Quare si sumatur $a=f^3\pm(3m+1)\alpha$, tum haec formula a^m-1 erit per $3m+1$ divisibilis. Q. E. D.

57. **Coroll. 1.** Ad valores ergo ipsius a inveniendos, omnia residua quae oriuntur, si cubi per $3m+1$ dividantur, notari debent. Unumquodque enim horum residuorum multiplo ipsius $3m+1$ quocunque auctum dabit valorem idoneum pro a.

58. **Coroll. 2.** Cum $3m+1$ esse debeat numerus primus, necesse est ut m sit numerus par, sicque numerus primus $3m+1$ unitate superabit multiplum senarii. Hinc erunt numeri pro m et $3m+1$ adhibendi sequentes:

m;	2,	4,	6,	10,	12,	14,	20,	22,	24,	26,	32,	etc.
$3m+1$;	7,	13,	19,	31,	37,	43,	61,	67,	73,	79,	97,	etc.

59. **Coroll. 3.** Si ergo numeri cubici per hos numeros primos $3m+1$ dividantur, sequentia residua remanebunt:

Divisores	Residua
7	1, 6
13	1, 5, 8, 12
19	1, 7, 8, 11, 12, 18
31	1, 2, 4, 8, 15, 16, 23, 27, 29, 30
37	1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36
	etc.

In his residuis primo occurrunt omnes cubi divisoribus minores, deinde si quodpiam residuum fuerit r pro divisore $3m+1$, tum quoque aliud dabitur residuum $=3m+1-r$; si enim cubus f^3 dederit residuum r, cubus $(3m+1-f)^3$ dabit residuum $-r$, seu $3m+1-r$.

60. **Scholion.** Notatu hic dignum est numerum residuorum perpetuo esse $=m$, si divisor fuerit $=3m+1$. Semper ergo dantur tres cubi, quorum radices sint $<3m+1$, ex quibus idem residuum resultat. Scilicet hi tres cubi 1^3, 2^3, 4^3 per 7 divisi idem dant residuum $=1$, et hi tres cubi 2^3, 5^3 et 6^3 per 13 divisi idem dant residuum 8. Praeterea hic notari convenit, si pro a alii valores, praeter hos assignatos capiantur, tum a^m-1 non esse per $3m+1$ divisibile, quod etsi verum esse facile deprehenditur, tamen ejus demonstratio ex praecedentibus non sequitur, pertinetque haec veritas ad id genus, quod nobis nosse, non autem demonstrare licet. His ergo casibus, quibus a^m-1 per $3m+1$ non est divisibile, haec formula $a^{2m}+a^m+1$ divisionem admittet.

61. **Theorema 13.** Si fuerit $a=f^n\pm(mn+1)\alpha$, existente $mn+1$ numero primo, tum haec forma a^m-1 erit divisibilis per $mn+1$.

Demonstratio. Ob $mn+1$ numerum primum erit $f^{mn}-1$ divisibile per $mn+1$. At est $f^{mn}-1=(f^n)^m-1$, unde quoque haec forma $(f^n\pm(mn+1)\alpha)^m-1$ erit divisibilis per $mn+1$. Quare si ponatur $a=f^n\pm(mn+1)\alpha$, haec formula a^m-1 per $mn+1$ dividi poterit. Q. E. D.

62. **Coroll. 1.** Si ergo potestates exponentis n per numerum primum $mn+1$ dividantur, singula residua vel ipsa, vel multiplo ipsius $mn+1$ quocunque aucta idoneos praebebunt valores pro a, ut a^m-1 fiat per $mn+1$ divisibile.

63. **Coroll. 2.** Hinc si a^m-1 non fuerit per $mn+1$ divisibile, tum valor ipsius a in hac expressione $f^n \pm (mn+1)\alpha$ non continebitur, seu nulla dabitur potestas exponentis n, quae per $mn+1$ divisa relinquat a.

64. **Scholion.** Propositionis hujus conversa, si omni modo examinetur, quoque vera deprehenditur; ita ut quoties a^m-1 sit divisibile per $mn+1$, toties quoque valor ipsius a in formula $f^n \pm (mn+1)\alpha$ contineatur; seu toties dabitur potestas f^n quae per $mn+1$ divisa relinquat a pro residuo. Ita cum observassem formulam $2^{64}-1$ esse per 641 divisibilem, ob $m=64$ fiet $n=10$, dabitur quoque potestas dignitatis decimae, quae per 641 divisa relinquat 2. Atque revera hujusmodi potestatem deprehendi esse 96^{10}. Praeterea vero cum $2^{32}-1$ non sit divisibile per 641, hoc casu fit $m=32$ et $n=20$; nulla igitur datur potestas dignitatis vicesimae, quae per 641 divisa relinquat 2. Veritas hujus posterioris asserti rigorose est evicta; sed adhuc desideratur demonstratio harum propositionum conversarum: scilicet si a^m-1 fuerit divisibile per numerum primum $mn+1$, tum quoque semper a esse numerum in hac formula $f^n \pm (mn+1)\alpha$ comprehensum. Atque si a non contineatur in formula $f^n \pm (mn+1)\alpha$, tum quoque a^m-1 per $mn+1$ divisionem non admittere. Quarum propositionum si altera demonstrari posset, simul veritas alterius esset evicta. Ceterum theorema hic demonstratum huc redit; ut quoties f^n-a fuerit divisibile per $mn+1$, toties quoque formula a^m-1 sit per $mn+1$ divisibilis. In hoc genere latius patet theorema sequens.

65. **Theorema 14.** Si fuerit f^n-ag^n divisibile per numerum primum $mn+1$, tum quoque a^m-1 erit divisibile per $mn+1$.

Demonstratio. Cum ponatur formula f^n-ag^n divisibilis per $mn+1$, erit quoque haec formula $f^{mn}-a^m g^{mn}$, quippe quae per illam dividi potest, divisibilis per $mn+1$. At cum $mn+1$ sit numerus primus, per eum divisibilis erit haec forma $f^{mn}-g^{mn}$; unde quoque differentia $g^{mn}(a^m-1)$, seu ipsa formula a^m-1 per $mn+1$ erit divisibilis, propterea quod g per $mn+1$ divisionem admittere nequeat, nisi simul f per eundem esset divisibile, qui casus in nostro ratiocinio perpetuo excluditur. Q. E. D.

66. **Coroll. 1.** Si ergo a^m-1 per $mn+1$ non fuerit divisibile, tum quoque nulli dantur numeri f et g, ut haec formula f^n-ag^n per $mn+1$ fiat divisibilis.

67. **Coroll. 2.** Si superioris propositionis conversa demonstrari posset, tum quoque evictum foret: quoties f^n-a per $mn+1$ dividi nequeat, tum ne hanc quidem formulam f^n-ag^n divisionem per $mn+1$ admittere posse, simul vero etiam pateret, si f^n-ag^n sit divisibile per $mn+1$, tum quoque dari hujusmodi formulam f^n-a, quae sit per $mn+1$ divisibilis.

68. **Theorema 15.** Si hujusmodi formula af^n-bg^n fuerit divisibilis per numerum primum $mn+1$, tum quoque haec formula a^m-b^m erit per $mn+1$ divisibilis.

Demonstratio. Si fuerit af^n-bg^n divisibile per $mn+1$, tum quoque erit haec formula $a^m f^{mn}-b^m g^{mn}$ per $mn+1$ divisibilis. At ob $mn+1$ numerum primum erit quoque haec formula

$f^{mn} - g^{mn}$, ideoque et haec $a^m f^{mn} - a^m g^{mn}$ per $mn+1$ divisibilis; subtrahatur haec ab illa $a^m f^{mn} - b^m g^{mn}$, atque residuum $g^{mn}(a^m - b^m)$, seu $a^m - b^m$ per $mn+1$ erit divisibile. Q. E. D.

69. **Coroll. 1.** Si itaque $a^m - b^m$ non fuerit per $mn+1$ divisibile, tum nulli dabuntur numeri pro f et g substituendi, ut hujusmodi formula $af^n - bg^n$ sit per $mn+1$ divisibilis.

70. **Coroll. 2.** Hujus propositionis conversa, quod, si fuerit formula $a^m - b^m$ divisibilis per $mn+1$, simul dentur numeri f et g, ut $af^n - bg^n$ fiat divisibilis per $mn+1$, utcunque examinetur, vera deprehenditur. Interim tamen ejus demonstratio etiamnum desideratur.

71. **Scholion.** Casus hujus propositionis inversae demonstrari potest, quo numeri m et n sunt inter se primi; hoc enim casu semper ejusmodi numeri μ et ν exhiberi possunt, ut sit $\mu n \pm 1 = \nu m$. Namque si inter numeros m et n ea operatio instituatur, quae pro maximo communi divisore institui solet, atque quoti notentur, ex iisque fractiones ad $\frac{m}{n}$ appropinquantes quaerantur, ultima erit $\frac{m}{n}$, et si penultima fuerit $\frac{\mu}{\nu}$ erit $\mu n \pm 1 = \nu m$. Hoc ergo lemmate praemisso demonstratio propositionis conversae, qua m et n sunt numeri inter se primi, ita se habebit.

72. **Theorema 16.** Si m et n fuerint numeri primi inter se, atque ista formula $a^m - b^m$ divisibilis sit per numerum $mn+1$, tum dabitur formula $af^n - bg^n$ divisibilis per $mn+1$.

Demonstratio. Ponatur $f = a^\mu$ et $g = b^\mu$, atque formula $af^n - bg^n$ abibit in hanc $a^{\mu n+1} - b^{\mu n+1}$; quare si μ ita capiatur, ut sit $\mu n + 1 = \nu m$, habebitur $a^{\nu m} - b^{\nu m}$, quae cum sit divisibilis per $a^m - b^m$, quoque per $mn+1$ divisibilis erit, sicque dabitur casus, quo $af^n - bg^n$ divisibile erit per $mn+1$. Sin autem fuerit $\mu n - 1 = \nu m$, tum sumatur $f = b^\mu$ et $g = a^\mu$, fietque

$$af^n - bg^n = ab^{\mu n} - ba^{\mu n} = ab\,(b^{\mu n-1} - a^{\mu n-1}) = -ab\,(a^{\nu m} - b^{\nu m})$$

ideoque erit per $mn+1$ divisibilis. Q. E. D.

73. **Coroll. 1.** Si ergo m et n fuerint numeri inter se primi, atque $mn+1$ numerus primus, tum istae propositiones sunt demonstratae: I. Si $af^n - bg^n$ fuerit divisibile per $mn+1$, tum quoque $a^m - b^m$ erit per $mn+1$ divisibile, et si illa formula nullo modo sit divisibilis per $mn+1$, tum etiam haec non erit divisibilis. II. Si $a^m - b^m$ fuerit divisibile per $mn+1$, tum dabitur numerus hujus formae $af^n - bg^n$ per $mn+1$ divisibilis, atque si $a^m - b^m$ per $mn+1$ divisionem non admittat, tum nullus dabitur numerus formae $af^n - bg^n$ per $mn+1$ divisibilis.

74. **Coroll. 2.** Si m sit numerus par, tum b aeque negative atque affirmative accipi potest; hoc ergo casu si $a^m - b^m$ fuerit divisibile per $mn+1$, tum etiam ejusmodi formula $af^n + bg^n$ per $mn+1$ divisibilis assignari poterit; id quod etiam inde patet, quod n sit numerus impar, ideoque potestas g^n negativa fieri queat.

75. **Coroll. 3.** Simili modo demonstrabitur, si fuerint ut ante m et n numeri inter se primi, atque haec formula $a^m - b^m$ sit divisibilis per $mn+1$, tum quoque exhiberi posse formulam hujusmodi $af^n - bg^n$ divisibilem per $mn+1$.

VIII.

Solutio problematis difficillimi a Fermatio propositi.

(N. Comment. II. 1749 p. 49. Exhib. 1748. Oct. 17.)

§ 1. Quamquam problemata, quae olim solutu difficilia sunt habita, hodie plerumque ob fines analyseos tantopere promotos nihil vel parum difficultatis habere solent; tamen hoc in eo problematum genere, quae ad methodum Diophanti pertinent, non usu venit. In hac enim analyseos parte post Fermatii tempora, qui plurimum studii et operae in ea fellicissimo cum successu consumsit, non solum nihil ultra praestitum esse videtur, sed etiam hoc studium a geometris, qui eum sunt secuti, fere penitus est neglectum. Etsi autem ea analyseos pars, in qua mathematici hodie potissimum versantur, ob summam utilitatem, quam ad reliquas scientias atque artes copiosissime affert, omni laude maxime digna est habenda: tamen altera quoque pars, quae in numeris est occupata, et ad problemata indeterminata solvenda adhiberi solet, idcirco minime est contemnenda, cum in ea plerumque summa ingenii vis cernatur atque ab analysta non mediocris sagacitas requiratur.

§ 2. Quae cum ita sunt comparata, ea hujus generis problemata, quae a Fermatio summopere difficilia sunt judicata, eadem et hodie non magis facta sunt facilia; hincque studium, quod in eorum solutione ponitur, non male collocatur. Proponit autem Fermatius in annotationibus suis ad Diophantum Bacheti sequens problema tanquam solutu difficillimum:

Invenire triangulum rectangulum in numeris rationalibus expressum, cujus uterque cathetus area ipsius trianguli minutus producat numerum quadratum.

Hujus ergo problematis sequentes, quas mihi quidem elicere contigit, solutiones in medium afferre visum est.

§. 3. **Praeparatio ad Solutionem.** Notum est triangulum rectangulum in numeris rationalibus exprimi, si ponatur cathetorum alter $= 2ab$, et alter $= aa - bb$, tum enim prodibit hypotenusa $= aa + bb$. Generalius catheti ambo poni possunt $\frac{2ab}{z}$ et $\frac{aa-bb}{z}$, prodeunte hypotenusa $= \frac{aa+bb}{z}$. Ponam autem, quoniam naturam trianguli rectanguli ultimo loco in computum vocare expedit,

$$\text{unum cathetum} = \frac{2x}{z}$$

$$\text{alterum cathetum} = \frac{y}{z}$$

$$\text{erit area} = \frac{xy}{zz}.$$

Ac primo per conditionem problematis hae quantitates

$$\left.\begin{array}{ll} \text{I. } \frac{2x}{z} - \frac{xy}{zz} & \text{seu } 2xz - xy \\ \text{II. } \frac{y}{z} - \frac{xy}{zz} & \text{seu } \quad yz - xy \end{array}\right\} \text{quadrata effici debent.}$$

Tum vero, quia hypotenusa fit $= \frac{\sqrt{(4xx+yy)}}{2}$, haec quantitas

III. $4xx + yy$ reddi debet quadratum.

§. 4. Quoniam hae ambae quantitates $2xz - xy$ et $yz - xy$ esse debent quadrata, earum productum pariter erit quadratum. Ordior ergo a producto

$$2xyzz - 2xxyz - xyyz + xxyy$$

quod quadratum reddi debet, ponoque ejus radicem $= xy - \frac{p}{q}yz$, ut ex evolutione valor ipsius z commode definiri queat; fiet autem

$$2xyzz - 2xxyz - xyyz + xxyy = xxyy - \frac{2p}{q}xyyz + \frac{pp}{qq}yyzz.$$

Ac deleto utrinque termino communi $xxyy$ et reliqua aequatione per yz divisa obtinebitur

$$2xz - 2xx - xy = \frac{-2p}{q}xy + \frac{pp}{qq}yz,$$

unde fit
$$z = \frac{2qqxx + qqxy - 2pqxy}{2qqx - ppy}.$$

§. 5. Invento jam valore ipsius z, fiet

$$2z - y = \frac{4qqxx - 4pqxy + ppyy}{2qqx - ppy} = \frac{(2qx - py)^2}{2qqx - ppy}$$

$$z - x = \frac{ppxy + qqxy - 2pqxy}{2qqx - ppy} = \frac{xy(p-q)^2}{2qqx - ppy}$$

hincque porro habebitur:

$$2xz - xy = \frac{x(2qx - py)^2}{2qqx - ppy} = \frac{xx(2qx - py)^2}{2qqxx - ppxy}$$

$$yz - xy = \frac{xyy(p-q)^2}{2qqx - ppy} = \frac{xxyy(p-q)^2}{2qqxx - ppxy}.$$

Quarum quantitatum cum utraque esse debeat quadratum, hoc efficietur, dummodo communis denominator: $2qqxx - ppxy$ fiat quadratum. Ponatur in hunc finem $2qqxx - ppxy = rrxx$, ac divisione facta per x erit $(2qq - rr)x = ppy$, et $\frac{x}{y} = \frac{pp}{2qq - rr}$.

§. 6. Sufficiet autem ad nostram solutionem nosse relationem inter x et y, quia in calculum jam introductus est communis denominator z, quare ponere licebit:

$$x = pp \text{ et } y = 2qq - rr,$$

unde fiet
$$z - x = \frac{pp(2qq - rr)(p-q)^2}{pprr},$$

ideoque
$$z = pp + \frac{(2qq - rr)(p-q)^2}{rr},$$

ideoque superest tantum, ut $4xx + yy$ reddatur quadratum, unde sequens expressio debet esse quadratum:
$$4p^4 + 4q^4 - 4qqrr + r^4,$$

unde sequentes solutiones particulares adornabuntur.

§ 7. **Solutio prima.** Quoniam igitur quaestio huc est reducta, ut pro litteris p, q, r ejusmodi valores assignentur, qui hanc expressionem

$$4p^4 + 4q^4 - 4qqrr + r^4$$

reddant quadratum, solutio generalis, quae omnes omnino valores idoneos harum litterarum complectatur, tradi nequit. Cum igitur solutionibus specialibus acquiescere debeamus, ponam primo

radicem hujus expressionis esse $= 2pp \mp rr$, ut termini $4p^4$ et r^4 utrinque se destruant, ac prodibit haec aequatio

$$4q^4 - 4qqrr = \mp 4pprr$$

unde fit $pp = \mp \frac{qq}{rr}(qq - rr)$, et habebimus

$$\text{vel } p = \frac{q}{r}\sqrt{(qq - rr)}, \quad \text{vel } p = \frac{q}{r}\sqrt{(rr - qq)}.$$

§ 8. Priori formulae $p = \frac{q}{r}\sqrt{(qq - rr)}$ satisfit ponendo $q = cc + dd$, et $r = 2cd$, unde fit $p = \frac{(cc + dd)(cc - dd)}{2cd}$.

Ex his ergo valoribus:

$$q = cc + dd; \quad r = 2cd; \quad p = \frac{(cc + dd)(cc - dd)}{2cd}$$

seu

$$p = (cc + dd)(cc - dd); \quad q = 2cd(cc + dd); \quad r = 4ccdd;$$

erit

$$x = pp; \quad y = 2qq - rr; \quad \sqrt{(4xx + yy)} = 2pp + rr; \quad z = x + \frac{y(p - q)^2}{rr};$$

quibus inventis erit pro triangulo rectangulo quaesito:

$$\text{I. cathetus} = \frac{2x}{z}, \qquad \text{II. cathetus} = \frac{y}{z}.$$

§ 9. **Exempl. 1.** Sit $c = 2$ et $d = 1$, ac prodibunt hi valores:

$$p = 5.3 = 15; \quad q = 4.5 = 20; \quad r = 4.4 = 16:$$

$$\text{unde} \quad x = 225; \quad y = 544; \quad z = 225 + \frac{544.25}{256} = \frac{25.89}{8} = \frac{2225}{8};$$

$$\text{atque} \quad \sqrt{(4xx + yy)} = 2pp + rr = 706.$$

Ex quibus conficitur hoc triangulum rectangulum in numeris:

$$\text{I. cath. } \frac{2x}{z} = \frac{144}{89}; \quad \text{II. cath. } \frac{y}{z} = \frac{4352}{25.89}; \quad \text{III. hypot.} = \frac{5648}{25.89};$$

area ergo erit $= \frac{72.4352}{25.89^2}$, et problemati ita satisfit:

$$\text{I. cath.} - \text{area} = \frac{144}{25.89^2}(25.89 - 2176) = \frac{144.49}{25.89^2} = \left(\frac{12.7}{5.89}\right)^2,$$

$$\text{II. cath.} - \text{area} = \frac{4352}{25.89^2}(89 - 72) = \frac{17.17.256}{25.89^2} = \left(\frac{16.17}{5.89}\right)^2.$$

§ 10. **Exempl. 2.** Sit $c = 3$ et $d = 1$, ac sequentes prodibunt valores

$$p = 10.8; \quad q = 6.10; \quad r = 6.6;$$

qui per 4 divisi ad minores terminos hos reducuntur

$$p = 20; \quad q = 15; \quad r = 9.$$

Ex his fit

$$x = 400; \quad y = 369; \quad z = \frac{4625}{9}; \quad \sqrt{(4xx + yy)} = 881;$$

unde triangulum rectangulum erit

I. cath. $\frac{2x}{z} = \frac{32.9}{185}$; II. cath. $\frac{y}{z} = \frac{81.41}{25.185}$; III. hyp. $= \frac{9.881}{25.185}$, atque area $= \frac{16.9.81.41}{25.185^2}$;

quare problemati ita satisfit:

$$\text{I. cath.} - \text{area} = \frac{2.16.9.25.185 - 16.9.81.41}{25.185^2} = \frac{16.9.5929}{25.185^2} = \left(\frac{4.3\ 77}{5.185}\right)^2,$$

$$\text{II. cath.} - \text{area} = \frac{81.41.185 - 16.9.81.41}{25.185^2} = \frac{81.41.41}{25.185^2} = \left(\frac{9.41}{5.185}\right)^2.$$

§ 11. **Solutio secunda.** Sumatur ex solutione praecedente casus posterior

$$p = \frac{q}{r}\sqrt{(rr-qq)},$$

qui requirit hos valores:

$$\left.\begin{aligned} r &= cc+dd \\ q &= 2cd \\ p &= \frac{2cd(cc-dd)}{cc+dd} \end{aligned}\right\} \text{ seu } \left\{\begin{aligned} r &= (cc+dd)^2; & x &= pp \\ q &= 2cd(cc+dd); & y &= 2qq-rr \\ p &= 2cd(cc-dd); & \sqrt{(4xx+yy)} &= 2pp-rr \end{aligned}\right.$$

et ut ante

$$z = x + \frac{y(p-q)^2}{rr}.$$

Quia autem esse debet

$$2qq > rr, \text{ erit } 8ccdd > (cc+dd)^2 \text{ et } 2cd\sqrt{2} > cc+dd,$$

seu $0 > cc - 2cd\sqrt{2} + dd$, quod huc redit, ut sit $dd > (c - d\sqrt{2})^2$; ergo

$$\text{vel } d > c - d\sqrt{2} \quad \text{seu} \quad \frac{d}{c} > \frac{1}{1+\sqrt{2}}$$

$$\text{vel } d > d\sqrt{2} - c \quad \text{seu} \quad \frac{d}{c} < \frac{1}{\sqrt{2}-1}.$$

Ergo si $d = 1$, necesse est ut sit vel $c < \sqrt{2}+1$, vel $c > \sqrt{2}-1$. At est $c > 1$, unde semper erit $c > \sqrt{2}-1$, et $2qq - rr$ fiet quantitas positiva. Erit itaque

$$\text{I. cath.} = \frac{2x}{z}; \quad \text{II. cath.} = \frac{y}{z} \quad \text{et III. hypot.} = \frac{\sqrt{(4xx+yy)}}{z}.$$

§ 12. **Exempl. I.** Sit $c = 2$ et $d = 1$, ac provenient hi valores:

$$\left.\begin{aligned} r &= 5.5 = 25 \\ q &= 4.5 = 20 \\ p &= 4.3 = 12 \end{aligned}\right\} \text{ hincque } \left\{\begin{aligned} x &= 144 \\ y &= 175 \\ \sqrt{(4xx+yy)} &= 337 \end{aligned}\right.$$

atque

$$z = 144 + \frac{175.64}{625} = \frac{4048}{25}.$$

Unde trianguli quaesiti erit

$$\text{I. cath.} = \frac{2x}{z} = \frac{288.25}{4048} = \frac{18.25}{253} = \frac{450}{253}$$

$$\text{II. cath.} = \frac{y}{z} = \frac{25.175}{4048} = \frac{4375}{4048}$$

$$\text{III. hypot.} = \frac{\sqrt{(4xx+yy)}}{z} = \frac{25.337}{4048} = \frac{8425}{4048}.$$

Area itaque erit

$$= \frac{225.4375}{253.4048} = \frac{225.4375}{16.253^2}.$$

Unde problemati hoc modo satisfit, ut sit:

$$\text{I. cath.} - \text{area} = \frac{225\,(32.253 - 4375)}{16.253^2} = \frac{225.61^2}{16.253^2} = \left(\frac{15.61}{4.253}\right)^2$$

$$\text{II. cath.} - \text{area} = \frac{25\,(175.253 - 9.4375)}{253.4048} = \frac{25.25.7.28}{16.253^2} = \left(\frac{25.14}{4.253}\right)^2.$$

§ 13. **Exempl. 2.** Sit $c = 3$ et $d = 1$, ac prodibunt hi valores:

$$\begin{array}{l|l} r = 10.10 & r = 25 \\ q = \ \ 6.10 & q = 15 \\ p = \ \ 6.\ 8 & p = 12 \end{array} \Bigg\}\ \text{hincque}\ \Bigg\{ \begin{array}{r} x = 144 \\ y = 175 \\ V(4xx + yy) = 337 \end{array}$$

qui valores cum sint iidem, qui in exemplo praecedente, hinc nulla nova oritur solutio. Majores autem numeros pro c et d non substituo, quod inde nimis complicati valores pro x, y et z prodeunt; praecipua enim cura in hoc debet poni, ut triangula in minimis, quantum fieri potest, numeris expressa reperiantur.

§ 14. **Solutio tertia.** Cum $4xx + yy = 4p^4 + 4q^4 - 4qqrr + r^4$ esse debeat quadratum, ejus radicem ponamus hic $= 2pp \pm 2qq$, ut sit $V(4xx + yy) = 2pp \pm 2qq$; atque prodibit haec aequatio $r^4 - 4qqrr = \pm 8ppqq$; unde fit $pp = \pm \frac{2rr\,(rr - 4qq)}{16qq}$ et vel $p = \frac{r}{4q} V(2rr - 8qq)$, vel $p = \frac{r}{4q} V(8qq - 2rr)$. Quia vero ob $y = 2qq - rr$ esse oportet $2qq > rr$, prior valor erit inutilis, habebimusque

$$p = \frac{r}{4q} V(8qq - 2rr); \quad x = pp; \quad y = 2qq - rr;$$

$$\text{et} \quad V(4xx + yy) = 2pp - 2qq$$

atque ut ante $z = x + \frac{y\,(p - q)^2}{rr}$. Erit ergo

$$\text{I. cath.} = \frac{2x}{z}; \quad \text{II. cath.} = \frac{y}{z}; \quad \text{III. hypot.} = \frac{V(4xx + yy)}{z}.$$

Nunc ergo huc devenimus, ut $8qq - 2rr$ reddatur quadratum: sit ejus radix $= \frac{c}{d}(2q + r)$ eritque $4q - 2r = \frac{cc}{dd}(2q + r)$, seu $4ddq - 2ddr = 2ccq + ccr$, hincque $q = cc + 2dd$ et $r = 4dd - 2cc$; $2q + r = 8dd$ atque $V(8qq - 2rr) = 8cd$, hincque $p = \frac{4cd\,(2dd - cc)}{2dd + cc}$. Quare in integris multiplicando per $2dd + cc$ fiet

$$\begin{array}{l|r} p = 4cd\,(2dd - cc) & x = pp \\ q = (2dd + cc)^2 & y = 2qq - rr \\ r = 2\,(2dd - cc)\,(2dd + cc) & V(4xx + yy) = 2pp - 2qq \end{array}$$

$$\text{atque} \qquad z = x + \frac{y\,(p - q)^2}{rr}.$$

§ 15. **Exempl. 1.** Sit $c = 1$, $d = 1$, erit:

$p = 4$; $\quad x = 16$;

$q = 9$; $\quad y = 126$;

$r = 6$; $\quad V(4xx + yy) = 130$; et $z = 16 + \frac{126.25}{36} = \frac{207}{2} = \frac{9.23}{2}$

$$\text{I. cath.} = \frac{64}{207}; \quad \text{II. cath.} = \frac{252}{207}; \quad \text{III. hypot.} = \frac{260}{207}$$

Area vero erit $= \frac{64.126}{207.207} = \frac{64.14}{9.23^2}$: sicque fiet

$$\text{I. cath.} - \text{area} = \frac{64}{9.23^2}(23 - 14) = \frac{64}{23^2} = \left(\frac{8}{23}\right)^2$$

$$\text{II. cath.} - \text{area} = \frac{252.23 - 64.14}{9.23^2} = \frac{28.175}{9.23^2} = \frac{4.7^2.5^2}{9.23^2} = \left(\frac{2.5.7}{3.23}\right)^2.$$

Hocque exemplum sine dubio in numeris minimis existit, uti deinceps ostendam.

§ 16. **Exempl. 2.** Quia debet esse $2qq > rr$, oportet ut sit $\frac{c}{d} > 2 - \sqrt{2}$; nihilque refert, sive sit $2dd > cc$, sive minus, quia nihil obstat, quominus p, q, r esse queant numeri negativi. Sit igitur $d = 2$, $c = 3$; erit $2dd - cc = -1$; $2dd + cc = 17$, atque

$p = -24.1 = -24$	$x = 576$
$q = 17.17 = 289$	$y = 2.7.41.17^2$
$r = -2.17 = -34$	$\sqrt{(4xx + yy)} = 2.5.53.313$, atque $z = \frac{90983}{2}$.

$$\text{I. Cath.} = \frac{2304}{90983}; \quad \text{II. cath.} = \frac{28.41.17^2}{90983}; \quad \text{III. hypot.} = \frac{4.5.53.313}{90983}.$$

§. 17. In his omnibus exemplis notari meretur, perinde esse, sive litterarum c et d valores capiantur affirmativi, sive negativi, inde enim tantum valores p, vel q, vel r prodeunt negativi; neque propterea valores x et y alterantur. Verum valor ipsius z variationem subit, ex quo pro z semper duplex valor assignari poterit, alter qui jam est exhibitus $z = x + \frac{y(p-q)^2}{rr}$, alter vero $z = x + \frac{y(p+q)^2}{rr}$: sicque ob duplicem valorem ipsius z singula exempla allata duplicabuntur.

§. 18. Hujusmodi solutiones particulares plures adhuc elicere licet, dum aliae idoneae quantitates pro radice quadrata hujus formae $4p^4 + 4q^4 - 4qqrr + r^4$ assumuntur. Veluti si haec radix ponatur $rr + 2qq \pm 2pp$, obtinebitur haec aequatio $-4qqrr = 4qqrr \pm 4pp(2qq + rr)$, seu $pp(2qq + rr) = \mp 2qqrr$; unde patet signum inferius valere, esseque $\sqrt{(4xx + yy)} = rr + 2qq - 2pp$, existente vel $p = \frac{2qr}{\sqrt{2(2qq + rr)}}$, vel $q = \frac{pr}{\sqrt{2(rr - pp)}}$, quae formulae jam facile rationales redduntur. Hic ergo si ponatur $r = 3$, $p = 1$, erit $q = \frac{3}{4}$, et in integris

$p = 4$	$x = 16$,
$q = 3$	$y = -126$
$r = 12$	$\sqrt{(4xx + yy)} = 130$.

qui casus, ob y negativum, non convenit quaestioni.

§ 19. Quoniam cardo quaestionis in hoc versatur, ut haec expressio reddatur quadratum: $4p^4 + (2qq - rr)^2$, potest hoc generaliter ita effici, ut ejus radix ponatur $= 2qq - rr + \frac{2m}{n}pp$,

$$\text{unde fiet} \quad pp = \frac{m}{n}(2qq - rr) + \frac{mm}{nn}pp, \quad \text{seu} \quad (nn - mm)pp = mn(2qq - rr),$$

$$\text{et } p = \sqrt{\frac{mn(2qq - rr)}{nn - mm}} = mn\sqrt{\frac{2qq - rr}{mn(nn - mm)}},$$

cui conditioni satisfiet ejusmodi numeros pro m et n quaerendo, ut sit $mn(nn - mm)$ numerus hujus formae $2ff - gg$. Verum haec solutio facilius obtinetur ex ipsa praeparatione ad solutionem

tradita, quae, si recte tractetur, omnes solutiones non solum in se complectitur, sed etiam solutiones in minoribus numeris omnes commode exhibet. Eam data opera evolvam.

§ 20. **Solutio generalis.** Assumtis cathetis trianguli quaesiti $\frac{2x}{z}$ et $\frac{y}{z}$ ponatur statim, ut anguli recti ratio habeatur:

$$x = ab; \quad y = aa - bb;$$

eritque trianguli

I. cath. $= \frac{2ab}{z}$; II. cath. $= \frac{aa-bb}{z}$; III. hypot. $= \frac{aa+bb}{z}$ et area hujus trianguli erit $= \frac{ab(aa-bb)}{zz}$.

Invenimus autem primo (§ 4.)

$$z = \frac{2qqxx + qqxy - 2pqxy}{2qqx - ppy},$$

$$\text{seu} \quad z = x + \frac{xy(p-q)^2}{2qqx - ppy}.$$

Vel, quia q tam negative quam affirmative accipere licet, erit

$$z = x + \frac{xy(p \pm q)^2}{2qqx - ppy}$$

existente $x = ab$ et $y = aa - bb$.

§ 21. Tum vero (§ 5.) hanc quantitatum x et y indolem invenimus, ut sit

$$2qqxx - ppxy = rrxx,$$

unde fit

$$z = x + \frac{y(p \pm q)^2}{rr} = ab + \frac{(aa-bb)(p \pm q)^2}{rr}.$$

Nihil aliud ergo efficiendum restat, nisi ut haec aequatio $2qqxx - ppxy = rrxx$, seu haec:

$$xy = \frac{xx}{pp}(2qq - rr)$$

conficiatur. Ubi cum sit $xy = ab(aa-bb)$, ejusmodi numeros pro a et b investigari oportet, ut fiat $ab(aa-bb)$ numerus hujus formae $2ff - gg$, seu $(2ff - gg)hh$.

§. 22. Ponamus igitur pro a et b jam hujusmodi valores esse erutos, ut sit

$$ab(aa-bb) = (2ff - gg)hh.$$

Cum igitur ob $x = ab$ sit:

$$(2ff - gg)hh = \frac{aabb}{pp}(2qq - rr),$$

hinc statim sponte se prodit

$$\frac{abq}{p} = fh \quad \text{et} \quad \frac{abr}{p} = gh.$$

Sit ergo $p = ab$, erit $q = fh$ et $r = gh$

atque $z = ab + \frac{(aa-bb)(ab \pm fh)^2}{gghh}$.

Eruntque trianguli rectanguli quaesiti latera:

$$\text{I. cath.} = \frac{2ab}{z} = \frac{2abgghh}{2abgghh + (aa-bb)(ab \pm fh)^2},$$

$$\text{II. cath.} = \frac{aa-bb}{z} = \frac{(aa-bb)gghh}{2abgghh + (aa-bb)(ab \pm fh)^2},$$

$$\text{III. hypot.} = \frac{aa+bb}{z} = \frac{(aa+bb)gghh}{2abgghh + (aa-bb)(ab \pm fh)^2}.$$

§. 23. Possunt etiam ex hujusmodi valoribus ipsarum a et b quibusvis innumerabilia triangula rectangula, quae quaesito satisfaciant, erui. Posito enim $p = ab$, si sit

$$ab(aa - bb) = (2ff - gg)hh,$$

erit $$(2ff - gg)hh = 2qq - rr$$

seu $$2(ffhh - qq) = gghh - rr.$$

Ponatur $2(fh + q) = \frac{m}{n}(gh + r)$, eritque $fh - q = \frac{n}{m}(gh - r)$, et hinc reperietur:

$$q = \frac{2mngh - (2nn + mm)fh}{2nn - mm}$$

$$r = \frac{(2nn + mm)gh - 4mnfh}{2nn - mm}.$$

Vel in numeris integris erit

$$p = (2nn - mm)ab$$
$$q = 2mngh - (2nn + mm)fh$$
$$r = (2nn + mm)gh - 4mnfh.$$

§ 24. Inventis sic valoribus his p, q et r, erit

$$z = \frac{abrr + (aa - bb)(p + q)^2}{rr}$$

atque trianguli quaesiti latera erunt:

I. cath. $= \frac{2ab}{z}$; II. cath. $= \frac{aa - bb}{z}$ et III. hypot. $= \frac{aa + bb}{z}$;

unde pro singulis idoneis valoribus ipsarum a et b, ut sit $ab(aa - bb) = (2ff - gg)hh$, ob m et n numeros pro arbitrio assumendos, innumerabilia triangula exhiberi poterunt.

§ 25. Quoniam igitur totum negotium huc redit, ut pro a et b ejusmodi numeri assumantur, ut productum $ab(aa - bb)$, sive $ab(a + b)(a - b)$ fiat numerus hujus formae $(2ff - gg)hh$. Quo hoc facilius effici possit, indolem numerorum, qui in hac forma generali $(2ff - gg)hh$, seu hac $2tt - uu$ continentur, attentius considerari conveniet. Ac primo quidem perspicuum est, in forma $2tt - uu$ contineri omnes numeros quadratos, quippe qui prodeunt, si $u = t$; tum vero etiam in hac forma continentur omnes numeri quadrati duplicati, ponendo $u = 0$. Praeterea vero infiniti alii occurrunt numeri, qui usque ad 200 sunt sequentes:

1, 2, 4, 7, 8, 9, 14, 16, 17, 18, 23, 25, 28, 31, 32, 34, 36, 41, 46, 47, 49, 50, 56, 62, 63, 64, 68, 71, 72, 73, 79, 81, 82, 89, 92, 94, 97, 98, 100, 103, 112, 113, 119, 121, 124, 126, 127, 128, 136, 137, 142, 144, 146, 151, 153, 158, 161, 162, 164, 167, 169, 175, 178, 184, 188, 191, 193, 194, 196, 199, 200.

§ 26. Si numeri primi considerentur, qui occurrunt, ii non solum omnes in hac forma $8m \pm 1$ continentur, sed etiam vicissim omnes numeri primi in hac gemina forma $8m \pm 1$ contenti ibi occurrunt, ideoque in forma $2tt - uu$ comprehenduntur. Praeterea vero horum numerorum primorum dupla adsunt, item eorum producta, tam per quosvis numeros quadratos, quam per se ipsos; nec non horum productorum dupla. Qua proprietate animadversa non difficile erit hos numeros quousque libuerit continuare.

§ 27. Hinc porro colligitur numeros non primos in forma $2tt - uu$ contentos alios divisores, qui quidem inter se sint primi, non admittere, nisi qui ipsi sint numeri in eadem forma $2tt - uu$ contenti. Quare cum productum $ab(a+b)(a-b)$ esse debeat numerus formae $2tt - uu$, bique factores a, b, $a+b$, $a-b$, sint vel primi inter se vel ad summum binarium pro communi divisore habeant, qui ipsi in forma $2tt - uu$ continetur, necesse est, ut hi singuli factores a, b, $a+b$, $a-b$ sint numeri ejusdem formae $2tt - uu$. Quo cognito ex tabula tradita non erit difficile idoneos valores pro a et b excerpere, ut non solum a et b, sed etiam $a+b$ et $a-b$ in eadem tabula existant.

§ 28. Quod si autem a, b, et $a+b$, $a-b$ singuli sint numeri formae $2tt - uu$, tum quoque eorum productum $ab(a+b)(a-b)$ in eadem forma continebitur, quod generatim ita ostendi potest: sint propositi duo numeri hujus formae, velut $2\alpha\alpha - \beta\beta$ et $2\gamma\gamma - \delta\delta$, erit eorum productum

$$(2\alpha\alpha - \beta\beta)(2\gamma\gamma - \delta\delta) = (2\alpha\gamma + \beta\delta)^2 - 2(\beta\gamma + \alpha\delta)^2$$
$$= 2(2\alpha\gamma + \beta\gamma + \alpha\delta + \beta\delta)^2 - (2\alpha\gamma + 2\beta\gamma + 2\alpha\delta + \beta\delta)^2;$$

est enim generaliter

$$xx - 2yy = 2(x+y)^2 - (x+2y)^2$$

ita ut hae duae formae $2tt - uu$ et $tt - 2uu$ inter se congruant. Cum igitur productum ex duobus numeris formae $2tt - uu$ facile ad eandem formam revocetur, etiam si quotcunque numeri hujus formae in se invicem multiplicentur, eorum productum in eadem forma comprehendi reperietur.

§ 29. Tribuatur ergo primo ipsi b valor quidam ex tabula numerorum allata (§ 25), et in eadem tabula facile dispicietur, utrum insint tres numeri $a-b$, a, $a+b$, qui differant illo numero b. Verum hanc tabulam inspicienti mox patet pro b vel numeros impares, vel per 8 divisibiles tantum assumi posse, siquidem a et b numeri debent esse inter se primi. Hujusmodi igitur valoribus pro b substitutis, pro a sequentes prodibunt valores:

b	valores ipsius a
1	8, 17, 63, 72, 127.
7	9, 16, 25, 144.
8	9, 17, 71, 81, 89, 161.
9	16, 23, 25, 32, 41, 73, 103, 112, 128, 137, 184.
16	25, 47, 63, 97, 137, 153.
17	64, 81, 144, 161.
23	41, 121, 144.
25	56, 72, 119, 128, 137, 144, 153, 169.
31	32, 63, 72, 81, 113, 144.
32	41, 49, 81, 121.
41	72, 103, 112, 153.

b	valores ipsius a
47	56, 72, 79, 81, 97, 128, 144.
49	72, 113, 146.
56	81, 97, 137.
63	64, 79, 136.
71	73.
72	79, 89, 97, 103, 119, 121.
73	89.
79	—
81	97, 112, 113.

§ 30. **Exempl. 1.** Quo usus hujus tabulae ad solutionem problematis clarius appareat, sit $b=1$, $a=8$, eritque:

$$ab=8;\quad aa-bb=63;\quad ab\,(aa-bb)=8.9.7=4.9.14;$$

fiet ergo $4.9.14=hh\,(2ff-gg)$, ideoque $h=6$ et $2ff-gg=14$, unde colligitur $f=3$, $g=2$, et ex § 23 obtinebimus

$$p=8\,(2nn-mn);\quad q=24mn-18\,(2nn+mm);\quad r=12\,(2nn+mm)-72mn;$$

qui, sublato communi divisore 2, erunt

$$p=8nn-4mm;\quad q=12mn-18nn-9mm;\quad r=12nn+6mm-36mn;$$

$$p+q=12mn-10nn-13mm;\quad -p+q=12mn-26nn-5mm;\quad \text{et}\quad z=8+\frac{63\,(p\pm q)^2}{rr}.$$

Hinc ergo innumerabiles prodeunt valores ipsius z, ex quorum quovis conficitur triangulum rectangulum

$$\text{I. cath.}=\frac{16}{z};\quad \text{II. cath.}=\frac{63}{z};\quad \text{III. hypot.}=\frac{65}{z}.$$

Casusque omnium simplicissimus oritur ponendo $n=0$ et $m=1$, unde fit $r=6$,

$$p-q=5;\quad p+q=-13$$

$$\text{et}\qquad z=8+\begin{cases}\frac{7}{4}\cdot 25\\ \frac{7}{4}\cdot 169\end{cases}$$

ergo vel $z=\frac{207}{4}$, vel $z=\frac{1215}{4}$, quorum valorum prior est pro casu simplicissimo jam § 15 exposito.

§ 31. **Exempl. 2.** Cum pro quibusque valoribus litterarum a et b infiniti exhiberi possint valores idonei ipsius z, quorum inventio nulla difficultate laborat per ea, quae §§ 23 et 24 sunt tradita, hic tantum valorem § 22 datum,

$$z=ab+\frac{(aa-bb)\,(ab+fh)^2}{gghh}$$

adhibere sufficiet, ob $ab(aa-bb)=(2ff-gg)hh$; unde erunt trianguli catheti,

$$\text{I.} = \frac{2ab}{z}; \quad \text{II.} = \frac{aa-bb}{z} \quad \text{et hypot.} = \frac{aa+bb}{z}.$$

Sit igitur $b=7$ et $a=9$, erit $ab=63$; $aa-bb=32$ et

$$ab(aa-bb)=63.32=16.9.14=(2ff-gg)hh,$$

unde fiet $h=12$; $f=3$ et $g=2$; ergo

$$z=63+\frac{32(63\pm 36)^2}{24.24}, \quad \text{seu} \quad z=63+\frac{9(7\pm 4)^2}{2};$$

ideoque vel $z=\frac{207}{2}$, vel $z=\frac{1215}{2}$; consequenter triangulum quaesitum erit ut ante:

$$\text{I. cath.} = \frac{252}{207}; \quad \text{II. cath.} = \frac{64}{207}; \quad \text{III. hypot.} = \frac{260}{207}.$$

§ 32. **Exempl. 3.** Quo usus tabulae § 29 exhibitae clarius perspiciatur, sumamus pro a et b majores numeros, sitque

$$b=41 \quad \text{et} \quad a=112, \text{ ut sit } ab=7.16.41; \quad aa-bb=71.9.17,$$

erit

$$ab(aa-bb)=16.9.7.17.41.71=(2ff-gg)hh, \quad \text{et} \quad h=12 \quad \text{atque} \quad 7.17.41.71=2ff-gg.$$

At est

$$7=3^2-2.1^2; \quad 17=2.3^2-1^2; \quad 41=7^2-2.2^2; \quad 71=2.6^2-1^2,$$

unde fit

$$7.41=(21\pm 2.2)^2-2(6\pm 7)^2=17^2-2.1^2=2.16^2-15^2;$$
$$17.71=(2.18\pm 1)^2-2(6\pm 3)^2=35^2-2.3^2=2.32^2-29^2.$$

Atque

$$7.17.41.71=(17.35-2.3)^2-2(51-35)^2=589^2-2.16^2;$$

ergo

$$7.17.41.71=2.573^2-557^2.$$

Haec autem reductio ad formam $2tt-uu$ infinitis aliis modis fieri potest, quorum simplicissimus est hic:

$$7.17.41.71=2.417^2-37^2 \quad \text{ut sit} \quad f=417 \quad \text{et} \quad g=37.$$

Ergo ob $h=12$, erit $fh=12.3.139$ et $gh=12.37$, ideoque

$$z=16.7.41+\frac{9.17.71(16.7.41\pm 4.9.139)^2}{16.9.37.37},$$

seu

$$z=16.7.41+\frac{17.71(4.7.41-9.139)^2}{37.37},$$

vel

$$z=16.7.41+\frac{17.71.103.103}{37.37}=\frac{19091511}{1369}.$$

Ex quo obtinebitur triangulum rectangulum:

$$\text{I. cath.} = \frac{9184.1369}{19091511}; \quad \text{II. cath.} = \frac{10863.1369}{19091511}; \quad \text{III. hypot.} = \frac{14225.1369}{19091511}.$$



IX.

De partitione numerorum.

(N. Comment. III. 1750 — 51. p. 125. Exhib. 1750. Jan. 26.)

§ 1. Problema *de partitione numerorum* primum mihi est propositum a celeb. professore Naude, in quo quaerebat, quot variis modis datus numerus integer, (hic enim perpetuo de numeris tantum integris et affirmativis est sermo), possit esse aggregatum duorum, vel trium, vel quatuor vel in genere quot libuerit numerorum. Sive, quod eodem redit, quaeritur, quot variis modis datus numerus vel in duas, vel tres, vel quatuor, vel quot libuerit partes dispertiri queat, unde huic problemati aptissime *partitionis numerorum* nomen est impositum. Bipartitum autem hoc problema a viro celeb. proponi solet: primo scilicet eos tantum partitionis modos postulat, quibus singulae partes, in quas numerus propositus resolvitur, sint inter se inaequales; tum vero hac inaequalitatis conditione omissa, omnes omnino partitionis modos requirit, sive partes quaepiam inter se fuerint aequales, sive omnes inaequales. Perspicuum autem est, hoc posteriori casu numerum partitionum plerumque multo esse majorem, quam priori, cum non solum omnes partitiones, quae casui priori satisfaciunt, simul posteriorem resolvant, sed etiam plerumque plures alii accedant, in quibus partes aequales contineantur.

§ 2. Ut vis problematis hujus clarius perspiciatur, nonnullos casus simpliciores afferam, qui actuali partitionum enumeratione facile expediuntur. Si quaeratur, quot variis modis numerus 6 in duas partes resolvi possit, statim apparet, hoc tribus modis fieri posse, cum sit:

$$6 = 1 + 5 = 2 + 4 = 3 + 3,$$

si quidem partium aequalitas non excludatur. Sin autem partes tantum inaequales desiderentur, ultima partitio $3 + 3$ est omittenda, hocque casu numerus 6 duobus tantum modis in duas partes inter se inaequales dispertiri potest. Quod si numerus impar, uti 9 proponatur, in duas partes distribuendus, quatuor prodibunt partitiones, quae sunt:

$$9 = 1 + 8 = 2 + 7 = 3 + 6 = 4 + 5,$$

ubi cum partes aequales non occurrant, numerus 9 quatuor modis in duas partes dispertietur, sive partes aequales excludantur, sive secus. Si plures duabus partes desiderentur, uti si quaeratur, quot variis modis numerus 12 in tres partes dispertiri possit, hoc sequentibus 12 modis fieri poterit:

$$12 = 1 + 1 + 10; \quad 12 = 1 + 2 + 9; \quad 12 = 1 + 3 + 8.$$
$$12 = 1 + 4 + 7; \quad 12 = 1 + 5 + 6; \quad 12 = 2 + 2 + 8.$$
$$12 = 2 + 3 + 7; \quad 12 = 2 + 4 + 6; \quad 12 = 2 + 5 + 5.$$
$$12 = 3 + 3 + 6; \quad 12 = 3 + 4 + 5; \quad 12 = 4 + 4 + 4.$$

Sin autem partes aequales excludantur, respondendum erit, numerum 12 tantum 7 modis in tres partes distribui posse.

§ 3. Hinc facile intelligitur, si tam numerus dispertiendus fuerit major, atque numerus partium, in quas eum resolvi oportet, ternarium quaternariumve superet, numerum partitionum tam fieri

magnum, ut per enumerationem actu instituendam difficillime obtineri queat. Neque etiam in hoc negotio inductioni multum est fidendum, quae, uti periculum facienti facile patebit, plerumque fallit, si ab enumeratione pro casibus simplicioribus facta ad magis compositos conclusiones formare voluerit. Sic ex methodo post explicanda patebit numerum 50 in septem partes, non exclusa partium aequalitate, dispertiri posse 8946 modis; sin autem partes aequales excludantur, remanebunt tantum 522 partitiones. Numerus porro 42 mille diversis modis in 20 partes omnino resolvi potest. At si quaeratur, quot variis modis numerus 125 in 12 partes, quae sint inter se omnes inaequales, distribui possit, reperietur hoc fieri posse 64707 modis.

§ 4. Quemadmodum hic omnes numeri integri partium loca tenere possunt, ita hoc problema in infinitum variari potest, prout numeri partes constituentes restringuntur. Ita aliud erit problema, si quaeratur, quot variis modis datus numerus n in p partes, quarum nulla datum numerum m excedat, resolvi possit. Partium quoque numerus omitti potest, uti si quaeratur, quot variis modis numerus 6 ex his numeris 1, 2, 3, 4, per additionem produci possit, quod sequentibus 9 modis fieri poterit:

$6 = 1 + 1 + 1 + 1 + 1 + 1$	$6 = 1 + 1 + 1 + 3$
$6 = 1 + 1 + 1 + 1 + 2$	$6 = 1 + 1 + 4$
$6 = 1 + 1 + 2 + 2$	$6 = 1 + 2 + 3$
$6 = 2 + 2 + 2$	$6 = 2 + 4$
	$6 = 3 + 3$

Vel etiam qualitas numerorum praescribi potest, qui partes constituant; uti si partes debeant esse vel numeri impares, vel quadrati, vel triangulares, vel alius cujusque generis. Sic si quaeratur, quot variis modis datus numerus possit esse summa quatuor quadratorum, quaestio ad hoc genus pertinebit. Jam pridem quoque partitio numerorum omnium in partes, quae sint termini hujus progressionis geometricae 1, 2, 4, 8, 16, 32, etc. est considerata, et quilibet numerus observatus est unico tantum modo ex his numeris 1, 2, 4, 8, 16, 32, etc. per additionem componi posse. Cujus quaestionis post Stifelium mentionem facit Schotenius in suis *Exercitationibus*, ubi ostendit pondera 1, 2, 4, 8, 16, 32, etc. librarum sufficere posse ad merces quotcunque librarum ponderandas. Neque vero ad hoc ostendendum alia methodo praeter inductionem utitur. Quamobrem non abs re erit veritatem hujus effati rigorose demonstrasse.

§ 5. Quem ad modum ergo haec aliaque similia problemata resolvi oporteat, hic ejusmodi methodum certam ac tutam proponam, ut inductione, cui vulgo ad solutionem istius modi quaestionum plurimum tribui solet, plane non sit opus. Utor ad hoc sequenti lemmate notissimo:

Si istud productum $(1 + az)(1 + bz)(1 + cz)(1 + dz)(1 + ez)$ *etc. sive factorum numerus sit finitus, sive infinitus, per actualem multiplicationem evolvatur, ut hujusmodi forma prodeat:*

$$1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

erit coefficiens secundi termini A *summa quantitatum omnium* a, b, c, d, e, *etc. Coefficiens vero* B *erit summa productorum ex binis harum quantitatum inaequalium. Coefficiens* C *erit summa productorum ex ternis istarum quantitatum inaequalibus et*

coefficiens D *erit summa productorum ex quaternis harum earundem quantitatum, et ita porro.*

In hujusmodi enim productis eadem quantitas, puta a, vel quaevis alia plus quam semel nusquam inesse potest. Unde hoc lemma mihi fundamentum suppeditat ad partitiones in partes inaequales.

§ 6. Sin autem inaequalitas partium non excludatur, adhibeo hoc lemma:

Si ista formula

$$\frac{1}{(1-az)(1-bz)(1-cz)(1-dz)(1-ez) \text{ etc.}}$$

sive factorum denominatorem constituentium numerus sit finitus, sive infinitus, post evolutionem denominatoris ope multiplicationis factam, per divisionem in seriem explicetur hujus formae:

$$1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

tum erit A *quidem ut ante summa quantitatum* a + b + c + d + e + etc. *At coefficiens* B *erit summa productorum ex binis harum quantitatum, non exclusa repetitione ejusdem quantitatis; erit scilicet:*

$$B = aa + ab + bb + ac + bc + cc + ad + bd + cd + dd + ae + \text{etc.}$$

Simili modo coefficiens C *erit summa productorum ex ternis harum quantitatum* a, b, c, d, e, *etc. factoribus aequalibus in quovis producto non exclusis. Atque eadem conditione adjecta erit coefficiens* D *summa productorum ex quaternis harum quantitatum, et ita porro.*

Hincque istud lemma viam aperiet ad partitiones, in quibus partium aequalitas non excluditur, absolvendas.

§ 7. Cum autem in problemate proposito non de productis, sed de summis numerorum quaestio instituatur, loco quantitatum a, b, c, d, e, etc. substituo potestates x^p, x^q, x^r, x^s, x^t, etc. Sic enim in productis ex binis ejusmodi occurrent potestates, quarum exponentes sint summae binarum ex serie p, q, r, s, t, etc. Simili modo producta ex ternis constantibus ejusmodi potestatibus, quarum exponentes sint summae trium numerorum ex eadem serie p, q, r, s, etc. Atque producta ex quaternis erunt potestates, quarum exponentes sint aggregata ex quaternis horum numerorum, et ita porro. Sicque quae ante de productis sunt notata, nunc ad summas transferuntur; et ita quidem, ut, si lemma prius adhibeatur, summae ex partibus tantum inaequalibus conflentur, sin autem lemma posterius in usum vocetur, partium aequalitas non excludatur. Hoc igitur modo ambo lemmata ad solutionem quaestionum ante memoratarum accommodari debebunt.

§ 8. Aggrediamur ergo hanc primum quaestionem:

Invenire quot variis modis datus numerus N *possit dispertiri in* p *partes, quae sint inter se inaequales.*

Quoniam huc omnes numeri integri affirmativi ad partes constituendas sunt idonei, pro serie superiorum exponentium accipienda est series numerorum naturalium: 1, 2, 3, 4, 5, 6, etc. Formetur ergo secundum lemma prius haec expressio:

$$s = (1 + xz)(1 + x^2 z)(1 + x^3 z)(1 + x^4 z)(1 + x^5 z) \text{ etc.}$$

in infinitum, quae multiplicatione actu instituta evolvatur in hanc seriem:

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

eritque

$$A = x^1 + x^2 + x^3 + x^4 + x^5 + x^6 + \text{etc.}$$

quod est aggregatum omnium potestatum ipsius x. Deinde quia B est summa productorum ex binis terminis inaequalibus seriei A, erit B summa potestatum ipsius x omnium, quarum exponentes sint aggregata duorum numerorum inaequalium; et cum eadem potestas saepius resultare possit, ea unciam habebit numericam indicantem, quot ea potestas modis sit productum ex duobus terminis seriei A, seu quot variis modis ejus exponens possit esse summa duorum numerorum inaequalium. Binis autem terminis seriei A re ipsa multiplicandis reperietur:

$$B = x^3 + x^4 + 2x^5 + 2x^6 + 3x^7 + 3x^8 + 4x^9 + 4x^{10} + \text{etc.}$$

Cujus seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adjunctae in duas partes inaequales dispertiri possit. Hac igitur serie in infinitum continuata, ope legis post eruendae, resolvitur problematis propositi casus, quo partitio in duas partes requiritur.

§ 9. Quantitas deinde C, cum contineat omnia producta, quae oriuntur ternis terminis inaequalibus seriei A invicem multiplicandis, constabit ex serie potestatum ipsius x, quarum exponentes sunt summae trium numerorum inter se inaequalium. Atque eadem potestas toties in ista serie C occurret, quoties ejus exponens ex tribus numeris inter se inaequalibus per additionem resultare poterit, reperieturque:

$$C = x^6 + x^7 + 2x^8 + 3x^9 + 4x^{10} + 5x^{11} + 7x^{12} + 8x^{13} + 10x^{14} + \text{etc.}$$

Cujus seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adjunctae in tres partes inaequales dispertiri possit, sic ex termino $8x^{13}$ colligitur, numerum 13 octo diversis modis in tres partes inaequales secari posse, quae sunt:

$13 = 1 + 2 + 10$	$13 = 2 + 3 + 8$
$13 = 1 + 3 + 9$	$13 = 2 + 4 + 7$
$13 = 1 + 4 + 8$	$13 = 2 + 5 + 6$
$13 = 1 + 5 + 7$	$13 = 3 + 4 + 6$

Ista igitur series C in infinitum continuata inserviet omnibus numeris in tres partes inaequales dispertiendis.

§ 10. Quantitas porro D, cum contineat omnia producta ex quaternis terminis inaequalibus seriei:

$$A = x^1 + x^2 + x^3 + x^4 + \text{etc.}$$

constabit serie potestatum ipsius x, quarum exponentes sint aggregata quatuor numerorum inter se inaequalium; et in hac serie quaelibet potestas ejusmodi habebit coefficientem, qui indicat, quot variis modis ejus exponens per additionem quatuor numerorum inter se inaequalium resultare possit. Reperietur autem:

$$D = x^{10} + x^{11} + 2x^{12} + 3x^{13} + 5x^{14} + 6x^{15} + 9x^{16} + 11x^{17} + \text{etc.}$$

Haec igitur series in infinitum continuata ostendet, quot variis modis quisque numerus possit esse summa quatuor numerorum inaequalium. Ex termino quippe $9x^{16}$ cognoscitur numerum 16 novem modis in quatuor partes inter se inaequales distribui posse.

§ 11. Si hoc modo ulterius progrediamur, patebit litteram E fore seriem potestatum ipsius x ita comparatam, ut cujusvis termini coefficiens indicet, quot variis modis exponens ipsius x in quinque partes inaequales dissecari possit. Erit autem:

$$E = x^{15} + x^{16} + 2x^{17} + 3x^{18} + 5x^{19} + 7x^{20} + 10x^{21} + 13x^{22} + \text{etc.}$$

Simili modo valor litterae F erit series partitionibus in sex partes inaequales inserviens, et litterae G, H, J, etc. pro partitionibus in partes septem, octo, novem etc. valebunt, eruntque:

$$F = x^{21} + x^{22} + 2x^{23} + 3x^{24} + 5x^{25} + 7x^{26} + 11x^{27} + 14x^{28} + \text{etc.}$$

$$G = x^{28} + x^{29} + 2x^{30} + 3x^{31} + 5x^{32} + 7x^{33} + 11x^{34} + 15x^{35} + \text{etc.}$$

etc.

Unde perspicitur primi cujusque seriei termini exponentem esse numerum trigonalem numeri partium propositi; tum vero tam hujus, quam secundi termini coefficientem esse $= 1$. Cujus quidem ratio facile intelligitur: minimus enim numerus, qui est summa septem numerorum inter se inaequalium, necessario est $= 1 + 2 + 3 + 4 + 5 + 6 + 7 = \frac{1}{2}.7.8 =$ numero trigonali ipsius septenarii; hicque numerus, pariter ac sequens unitate major, plus uno modo in septem partes inaequales dispertiri nequit.

§ 12. Totum ergo negotium redit ad commodam serierum B, C, D, E, F, etc. formationem, ne id ipsum, quod quaeritur, scilicet partitionum numerus ad cujusque seriei formationem adhibeatur. Ac primo quidem lex progressionum A et B est aperta, cum prioris coefficientes sint omnes unitates, posterioris vero termini seriei numerorum naturalium geminati: sequentium vero serierum lex minus est aperta, et quousque eas hic continuavimus, coefficientes ex ipsis cujusque exponentis partitionibus constituimus. Alio itaque modo valores istarum litterarum A, B, C, D, etc. investigari oportet, unde haec exoritur quaestio: Invenire valores litterarum A, B, C, D, E, etc. ita ut summa hujus seriei:

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

aequalis fiat isti expressioni:

$$s = (1 + xz)(1 + x^2z)(1 + x^3z)(1 + x^4z)(1 + x^5z) \text{ etc.}$$

Hunc in finem igitur perpendendus est nexus, qui inter has duas expressiones intercedit, et quem ad modum altera immutari debeat, si in altera mutatio instituatur.

§ 13. Quia utriusque expressionis idem est valor s, ambae inter se manebunt aequales, si in utraque loco z scribatur quaecunque alia quantitas. Ponamus igitur in utraque xz loco z, et valor utrinque resultans vocetur $= t$, eritque primo:

$$t = 1 + Axz + Bx^2z^2 + Cx^3z^3 + Dx^4z^4 + \text{etc.}$$

tum vero altera expressio transmutabitur in hanc:

$$t = (1 + x^2z)(1 + x^3z)(1 + x^4z)(1 + x^5z) \text{ etc.}$$

qui posterior ipsius t valor, si cum posteriore valore ipsius s comparetur, quo erat:

$$s = (1 + xz)(1 + x^2z)(1 + x^3z)(1 + x^4z) \text{ etc.}$$

mox patebit esse $s = (1 + xz)\,t$. Quae relatio cum etiam in alteris valoribus ipsarum s et t locum habere debeat, nobis praebebit hanc aequationem:

$$\begin{array}{rl} s = & 1 + Az + Bz^2 + Cz^3 + Dz^4 + \text{etc.} \\ \hline (1+xz)\,t = & 1 + Axz + Bx^2z^2 + Cx^3z^3 + Dx^4z^4 + \text{etc.} \\ & + xz + Ax^2z^2 + Bx^3z^3 + Cx^4z^4 + \text{etc.} \end{array}$$

Unde terminis homogeneis inter se aequandis, fiet:

$$A = \frac{x}{1-x}$$

$$B = \frac{Ax^2}{1-x^2} = \frac{x^3}{(1-x)(1-x^2)}$$

$$C = \frac{Bx^3}{1-x^3} = \frac{x^6}{(1-x)(1-x^2)(1-x^3)}$$

$$D = \frac{Cx^4}{1-x^4} = \frac{x^{10}}{(1-x)(1-x^2)(1-x^3)(1-x^4)}$$

$$E = \frac{Dx^5}{1-x^5} = \frac{x^{15}}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)}$$

etc.

§ 14. Series ergo, quae supra pro litteris A, B, C, D, E, etc. prodire observatae sunt, oriuntur ex evolutione fractionum, quas hic invenimus, unde constat, seriem A esse geometricam, nempe $A = x + x^2 + x^3 + x^4 + x^5 +$ etc. quae, quod quidem est planissimum, indicat quemque numerum unico modo ex uno numero integro constare. Reliquae vero series B, C, D, E, etc. sunt recurrentes, quarum scala relationis ex cujusvis fractionis denominatore per multiplicationem evoluto patebit. Ad hoc ostendendum negligamus tantisper numeratores, qui sunt potestates ipsius x, quarum exponentes sunt numeri trigonales, earumque loco scribamus unitatem. Sit igitur

$$\frac{A}{x} = 1 + \alpha' x + \beta' x^2 + \gamma' x^3 + \delta' x^4 + \varepsilon' x^5 + \ldots\ldots + \nu' x^n = \mathfrak{A}$$

$$\frac{B}{x^3} = 1 + \alpha'' x + \beta'' x^2 + \gamma'' x^3 + \delta'' x^4 + \varepsilon'' x^5 + \ldots\ldots + \nu'' x^n = \mathfrak{B}$$

$$\frac{C}{x^6} = 1 + \alpha''' x + \beta''' x^2 + \gamma''' x^3 + \delta''' x^4 + \varepsilon''' x^5 + \ldots\ldots + \nu''' x^n = \mathfrak{C}$$

$$\frac{D}{x^{10}} = 1 + \alpha^{IV} x + \beta^{IV} x^2 + \gamma^{IV} x^3 + \delta^{IV} x^4 + \varepsilon^{IV} x^5 + \ldots\ldots + \nu^{IV} x^n = \mathfrak{D}$$

$$\frac{E}{x^{15}} = 1 + \alpha^{V} x + \beta^{V} x^2 + \gamma^{V} x^3 + \delta^{V} x^4 + \varepsilon^{V} x^5 + \ldots\ldots + \nu^{V} x^n = \mathfrak{E}$$

$$\frac{F}{x^{21}} = 1 + \alpha^{VI} x + \beta^{VI} x^2 + \gamma^{VI} x^3 + \delta^{VI} x^4 + \varepsilon^{VI} x^5 + \ldots\ldots + \nu^{VI} x^n = \mathfrak{F}$$

etc.

§ 15. Solutio ergo quaestionis ad inventionem serierum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$, etc. reducitur, quas patet singulas esse recurrentes. Ac primo quidem series $\mathfrak{A}$, cum sit $\mathfrak{A} = \frac{1}{1-x}$, est adeo geometrica, atque $\alpha' = 1$, $\beta' = 1$, $\gamma' = 1$, $\delta' = 1$, etc. quod per se est perspicuum. Series autem $\mathfrak{B}$, cum sit

$$\mathfrak{B} = \frac{1}{(1-x)(1-x^2)} = \frac{1}{1 - x - x^2 + x^3},$$

erit recurrens, scala relationis existente $+1$, $+1$, -1; unde erit:

$$\alpha'' = 1,$$
$$\beta'' = \alpha'' + 1,$$
$$\gamma'' = \beta'' + \alpha'' - 1,$$
$$\delta'' = \gamma'' + \beta'' - \alpha'',$$
$$\varepsilon'' = \delta'' + \gamma'' - \beta'',$$
$$\zeta'' = \varepsilon'' + \delta'' - \gamma'',$$
etc.

Simili modo series $\mathfrak{C}$, ob

$$\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)} = \frac{1}{1-x-x^2+x^4+x^5-x^6},$$

erit recurrens et scalam relationis habebit $+1, +1, 0, -1, -1, +1$. Unde erit:

$$\alpha''' = 1$$
$$\beta''' = \alpha''' + 1$$
$$\gamma''' = \beta''' + \alpha''' + *$$
$$\delta''' = \gamma''' + \beta''' + * - 1$$
$$\varepsilon''' = \delta''' + \gamma''' + * - \alpha''' - 1$$
$$\zeta''' = \varepsilon''' + \delta''' + * - \beta''' - \alpha''' + 1$$
$$\eta''' = \zeta''' + \varepsilon''' + * - \gamma''' - \beta''' + \alpha'''$$
$$\vartheta''' = \eta''' + \varepsilon''' + * - \delta''' - \gamma''' + \beta'''$$
etc.

Eodem modo series sequentes perspicientur esse recurrentes, singularumque scalae relationis hoc modo assignari poterunt. Etsi autem hoc pacto istae series non difficulter formari possunt, tamen ista ratione relicta mox multo commodiorem modum exhibebo, harum serierum quamvis ex praecedente formandi, postquam observationem maximi momenti communicavero.

§ 16. Cum sit $\mathfrak{B} = \frac{1}{(1-x)(1-x^2)}$, patet in serie evoluta $\mathfrak{B}$ quamvis potestatem ipsius x toties occurrere debere, quoties ea ex potestatibus x^1, x^2 per multiplicationem oriri potest, seu quoties ejus exponens ex numeris 1 et 2 per additionem produci potest. Ita cum sit:

$$\mathfrak{B} = 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + \ldots\ldots\ldots + v''x^n$$

ex termino $3x^4$ intelligitur, numerum 4 tribus modis ex numeris 1 et 2 per additionem oriri posse, qui sunt:

$$4 = 1+1+1+1; \quad 4 = 1+1+2; \quad \text{et} \quad 4 = 2+2.$$

In genere ergo terminum $v''x^n$ considerando, coefficiens v'' indicabit, quot modis exponens n ex numeris 1 et 2 per additionem produci possit. Cum igitur sit $B = \mathfrak{B}x^3$, in serie B habebitur iste terminus $v''x^{n+3}$, qui cum indicet, numerum $n+3$ tot variis modis in duas partes inaequales secari posse, quot unitates coefficiens v'' in se complectatur, manifestum est, numerum $n+3$ tot modis in duas partes inaequales distribui posse, quot modis numerus n ex numeris 1 et 2 per additionem produci queat.

§ 17. Deinde cum sit $\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)}$, patet in hac serie $\mathfrak{C}$ quamvis potestatem ipsius x toties occurrere debere, quoties ea ex potestatibus x^1, x^2, x^3 per multiplicationem oriri

queat, seu quod idem est, quoties ejus exponens ex numeris 1, 2, 3 per additionem produci possit: Ita cum sit:

$$\mathfrak{C} = 1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 7x^6 + \ldots\ldots + v''' x^n,$$

ex quovis ejus termino $5x^5$ cognoscetur, exponentem 5 quinque modis ex numeris 1, 2, 3 per additionem produci posse, qui sunt:

$5 = 1 + 1 + 1 + 1 + 1$; $5 = 1 + 1 + 1 + 2$; $5 = 1 + 1 + 3$; $5 = 1 + 2 + 2$; $5 = 2 + 3$.

In genere autem terminum $v''' x^n$ considerando, coefficiens v''' indicabit, quot variis modis numerus n ex numeris 1, 2, 3, per additionem oriri queat. Cum igitur sit $C = \mathfrak{C} x^6$, in serie C habebitur iste terminus $v''' x^{n+6}$ quo indicatur, numerum $n + 6$ tot modis, quot unitates continentur in coefficiente v''', in tres partes inaequales dispertiri posse. Unde consequitur, numerum $n + 6$ totidem modis in tres partes inaequales distribui posse, quot modis numerus 6 ex numeris 1, 2, 3 per additionem produci possit.

§ 18. Non opus est, ut hoc ratiocinium longius prosequamur, cum hinc jam abunde perspiciatur, quemvis numerum $n + 10$ tot variis modis in quatuor partes inaequales dispertiri posse, quot modis numerus n ex his quatuor numeris 1, 2, 3, 4 per additionem produci possit. Simili modo quilibet numerus $n + 15$ tot variis modis in quinque partes inaequales dispertiri poterit, quot modis numerus n ex his quinque numeris 1, 2, 3, 4, 5 per additionem produci potest. Generatim ergo numerus $n + \frac{m(m+1)}{2}$ tot variis modis in m partes inaequales dispertiri poterit, quot variis modis numerus n ex his numeris 1, 2, 3, 4......m per additionem produci potest. Quod si ergo quaeratur, quot variis modis numerus N in m partes inaequales dispertiri possit, responsio reperietur, si casuum numerus investigetur, quibus numerus $N - \frac{m(m+1)}{2}$ ex numeris 1, 2, 3, 4........m per additionem produci potest.

§ 19. Hoc igitur modo resolutio quaestionis propositae, de partitione cujusque numeri in quot libuerit partes inaequales, reducitur ad solutionem alius problematis jam supra commemorati, quo quaeritur, quot variis modis quilibet numerus ex aliquot terminis hujus progressionis arithmeticae 1, 2, 3, 4, 5, etc. per additionem produci possit. Hacque posteriore quaestione resoluta simul prior resolvetur. Quod ut clarius explicemus, nova signa ad commodiorem expressionem adhibeamus. Denotet ergo haec scriptio:

$n^{(2)}$ numerum casuum, quibus numerus n ex duobus numeris 1, 2 per additionem formari possit;

$n^{(3)}$ denotet numerum casuum, quibus numerus n ex his numeris 1, 2, 3 per additionem formari possit;

et $n^{(m)}$ denotet numerum casuum, quibus numerus n ex his numeris 1, 2, 3.....m per additionem produci possit. Cum igitur valores hujusmodi characterum fuerint definiti, quod deinceps praestabimus, problema propositum ita resolvetur. Si quaeratur scilicet, quot variis modis numerus N in m partes inaequales dispertiri possit, numerus casuum quaesitus exprimetur hoc charactere

$$\left(N - \frac{m(m+1)}{1.2}\right)^{(m)},$$

quippe quo indicatur, quot variis modis numerus $N - \frac{m(m+1)}{2}$ ex his numeris $1, 2, 3, \ldots m$ per additionem produci possit.

§ 20. Ad hanc eandem quaestionem quoque reducitur solutio alterius problematis a celeb. Naudeo propositi, quam ob rem expediet, et hoc problema ante resolvi, quam ampliorem characterum modo assumtorum evolutionum suscipiamus, sic enim tria problemata, quae inter se maxime videantur diversa, una eademque opera resolvemus. Problema autem ita se habet:

Invenire quot variis modis datus numerus N *possit dispertiri in* p *partes, partium aequalitate non exclusa.*

Quoniam hic partium aequalitas non excluditur, sequentem formam contemplabor, quae hujus quaestionis solutionem in se continebit

$$s = \frac{1}{(1-xz)(1-x^2z)(1-x^3z)(1-x^4z)(1-x^5z)\text{ etc.}}$$

quae secundum potestates ipsius z evoluta praebeat hanc seriem:

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

eritque, ut supra § 6 notavimus, coefficiens A summa omnium terminorum hujus seriei

$$x,\ x^2,\ x^3,\ x^4,\ x^5,\ \text{etc.}$$

seu

$$A = x^1 + x^2 + x^3 + x^4 + x^5 + x^6 + \text{etc.}$$

quae est eadem series, quam in solutione praecedentis problematis pro littera A obtinuimus.

§ 21. Deinde vero est B summa productorum ex binis terminis seriei A, quadratis singulorum terminorum non exclusis. Hinc erit B summa omnium potestatum ipsius x, quarum exponentes sint aggregata duorum numerorum, sive aequalium, sive inaequalium: et cum eadem potestas hoc modo saepius resultare possit, ea unciam habebit numericam indicantem, quot ea potestas modis sit productum ex binis terminis seriei A; seu quot variis modis ejus exponens possit esse summa duorum numerorum, tam aequalium, quam inaequalium. Ex hoc fonte reperietur:

$$B = x^2 + x^3 + 2x^4 + 2x^5 + 3x^6 + 3x^7 + 4x^8 + 4x^9 + \text{etc.}$$

cujus seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adjunctae in duas partes dispertiri possit. Hac igitur serie in infinitum continuata, problematis propositi casus, quo partitio in duas partes requiritur, facile resolvitur.

§ 22. Quantitas porro C, cum contineat omnia producta, quae oriuntur terminis ternis seriei A, sive inaequalibus, sive aequalibus, invicem multiplicandis, constabit ex serie potestatum ipsius x, quarum exponentes sint summae trium numerorum integrorum affirmativorum. Atque eadem potestas x^n toties in serie C occurret, quoties ejus exponens n ex tribus numeris, sive aequalibus, sive inaequalibus, per additionem resultare potest. Erit autem:

$$C = x^3 + x^4 + 2x^5 + 3x^6 + 4x^7 + 5x^8 + 7x^9 + 8x^{10} + 10x^{11} + \text{etc.}$$

cujus seriei quilibet coefficiens indicat, quot variis modis exponens potestatis ipsius x adjunctae in

tres partes, sive aequales, sive inaequales dispertiri possit. Sic ex termino $8x^{10}$ colligitur, numerum 10 octo modis diversis in tres partes secari posse, quae partitiones sunt:

$10 = 1 + 1 + 8$	$10 = 2 + 2 + 6$
$10 = 1 + 2 + 7$	$10 = 2 + 3 + 5$
$10 = 1 + 3 + 6$	$10 = 2 + 4 + 4$
$10 = 1 + 4 + 5$	$10 = 3 + 3 + 4$

Ista igitur series C in infinitum continuata omnibus numeris in tres partes dispertiendis inserviet.

§ 23. Simili modo quantitas D, cum contineat omnia producta ex quatuor terminis seriei

$$A = x + x^2 + x^3 + x^4 + \text{etc.}$$

ejusdem termini repetitione non exclusa, constabit serie potestatum ipsius x, quarum exponentes sint aggregata quatuor numerorum, sive aequalium, sive inaequalium. In hac igitur serie quaelibet potestas ipsius x ejusmodi habebit coefficientem, qui indicet, quot variis modis ejus exponens per additionem 4 numerorum resultare possit. Reperietur autem hinc:

$$D = x^4 + x^5 + 2x^6 + 3x^7 + 5x^8 + 6x^9 + 9x^{10} + 11x^{11} + \text{etc.}$$

Haec igitur series in infinitum continuata ostendet, quot variis modis quilibet numerus in quatuor partes dispertiri possit. Sic ex termino $9x^{10}$ concluditur numerum 10 novem modis in quatuor partes dispertiri posse, quae partitiones sunt:

$10 = 1 + 1 + 1 + 7$	$10 = 1 + 1 + 4 + 4$	$10 = 1 + 3 + 3 + 3$
$10 = 1 + 1 + 2 + 6$	$10 = 1 + 2 + 2 + 5$	$10 = 2 + 2 + 2 + 4$
$10 = 1 + 1 + 3 + 5$	$10 = 1 + 2 + 3 + 4$	$10 = 2 + 2 + 3 + 3$

§ 24. Hoc modo ulterius procedendo patebit, litteram E fore seriem potestatum ipsius x ita comparatam, ut cujusvis termini coefficiens indicet, quot variis modis exponens ipsius x in quinque partes dispertiri possit. Erit autem:

$$E = x^5 + x^6 + 2x^7 + 3x^8 + 5x^9 + 7x^{10} + 10x^{11} + 13x^{12} + \text{etc.}$$

Pari modo valor litterae F erit series partitionibus in sex partes inserviens, et litterarum G, H, J, etc. valores pro partitionibus in partes septem, octo, novem, etc. valebunt, erit autem:

$$F = x^6 + x^7 + 2x^8 + 3x^9 + 5x^{10} + 7x^{11} + 11x^{12} + 14x^{13} + \text{etc.}$$

$$G = x^7 + x^8 + 2x^9 + 3x^{10} + 5x^{11} + 7x^{12} + 11x^{13} + 15x^{14} + \text{etc.}$$

etc.

Si hae series cum illis comparentur, quas in solutione superioris problematis pro iisdem litteris invenimus, mox patebit totum discrimen tantum in potestatibus ipsius x constare, coefficientesque solos utrinque similiter procedere. Ne autem hic inductioni ullum locum concedamus, istam convenientiam sequenti demonstratione evincemus.

§ 25. Consideremus, ut supra, duos valores ipsius s, qui sunt:

$$s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

$$s = \frac{1}{(1-xz)(1-x^2z)(1-x^3z)(1-x^4z)(1-x^5z)\ \text{etc.}}$$

qui, si loco z ubique ponatur xz, abeant in t, eritque:

$$t = 1 + Axz + Bx^2z^2 + Cx^3z^3 + Dx^4z^4 + Ex^5z^5 + \text{etc.}$$

$$t = \frac{1}{(1-x^2z)(1-x^3z)(1-x^4z)(1-x^5z)\ \text{etc.}}$$

Unde si posteriores ipsarum s et t valores invicem comparentur, mox patet esse $s = \frac{t}{1-xz}$, seu $t = (1-xz)s$, quae eadem relatio cum quoque inter priores litterarum s et t valores locum tenere debeat, erit:

$$t = 1 + Axz + Bx^2z^2 + Cx^3z^3 + Dx^4z^4 + Ex^5z^5 + \text{etc.} =$$

$$(1-xz)s = 1 + Az + Bz^2 + Cz^3 + Dz^4 + Ez^5 + \text{etc.}$$

$$- xz - Axz^2 - Bxz^3 - Cxz^4 - Dxz^5 - \text{etc.}$$

Unde per coaequationem terminorum homogeneorum invenitur:

$$A = \frac{x}{1-x}$$

$$B = \frac{Ax}{1-xx} = \frac{x^2}{(1-x)(1-x^2)}$$

$$C = \frac{Bx}{1-x^3} = \frac{x^3}{(1-x)(1-x^2)(1-x^3)}$$

$$D = \frac{Cx}{1-x^4} = \frac{x^4}{(1-x)(1-x^2)(1-x^3)(1-x^4)}$$

etc.

§ 26. Ex his formulis intelligitur, istas series non solum quoque esse recurrentes, uti superiores, sed etiam coefficientium utrinque eandem esse legem. Quare si neglectis numeratoribus ponatur:

	ut sit
$\mathfrak{A} = \frac{1}{1-x}$	$A = \mathfrak{A}x$
$\mathfrak{B} = \frac{1}{(1-x)(1-x^2)}$	$B = \mathfrak{B}x^2$
$\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)}$	$C = \mathfrak{C}x^3$
$\mathfrak{D} = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)}$	$D = \mathfrak{D}x^4$
etc.	etc.

Partitio cujusque numeri in partes quotcunque, sive aequales, sive inaequales, pendet a formatione serierum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc. quae, uti ante observavimus, indicant, quot variis modis quivis numerus ex aliquot terminis initialibus hujus seriei 1, 2, 3, 4, 5, etc. per additionem produci queat. Sic cum sit $B = \mathfrak{B}x^2$, quivis numerus $n+2$ totidem modis in duas partes dispertiri potest, quot modis numerus n ex numeris 1 et 2 per additionem produci potest. Simili modo cum sit $C = \mathfrak{C}x^3$, numerus $n+3$ tot modis in tres partes dispertietur, quot modis numerus n per additionem ex

numeris 1, 2, 3 componi poterit. Atque generaliter numerus $n+m$ tot variis modis in m partes, sive aequales, sive inaequales dispertiri potest, quot modis numerus n ex numeris 1, 2, 3,....m per additionem produci potest.

§ 27. Pendet ergo et hoc problema a solutione quaestionis, qua quaeritur, quot variis modis datus numerus ex aliquot terminis initialibus hujus seriei 1, 2, 3, 4, etc. per additionem resultare possit. Si igitur, ut supra, haec scribendi formula $N^{(m)}$ denotet numerum modorum, quibus numerus N ex numeris 1, 2, 3,........m per additionem componi potest, seu quibus numerus N in partes quotcunque distribui possit, quarum nulla major sit numero m; hujus modi characteribus et hoc problema propositum resolvi poterit. Scilicet $n^{(m)}$ indicabit, quot variis modis numerus $n+m$ in m partes, sive aequales, sive inaequales dispertiri possit. Hinc si quaeratur, quot modis numerus N in partes m, sive aequales, sive inaequales distribui possit, numerum modorum quaesitum indicabit haec formula $(N-m)^{(m)}$. Si igitur hoc problema cum praecedente conferatur, perspicuum erit numerum $n+m$ totidem modis in m partes, sive aequales, sive inaequales distribui posse, quot modis numerus $n+\frac{m(m+1)}{2}$ in m partes inaequales dispertiri possit.

§ 28. Solutio ergo amborum problematum a cel. Naudeo propositorum huc revocatur, ut definiatur, quot variis modis numerus quicunque n ex his numeris 1, 2, 3,........m per additionem produci possit; seu ut investigetur valor characteris $n^{(m)}$. Quemadmodum ergo hoc novum problema ex formulis jam ante inventis commodissime resolvi queat, videamus. Ac primo quidem, si sit $m=1$, quia quilibet numerus unico modo ex meris unitatibus per additionem elici potest, erit $n^{(1)}=1$, quod idem prima formula $\mathfrak{A}=\frac{1}{1-x}$, seu series inde formata:

$$\mathfrak{A}=1+x+x^2+x^3+x^4+x^5+\text{etc.}$$

manifesto indicat.

§ 29. Quoniam series $\mathfrak{B}=\frac{1}{(1-x)(1-x^2)}$ indicat, quot modis quisque numerus ex numeris 1 et 2 per additionem formari possit, in hac serie potestatis x^n coefficiens erit $=n^{(2)}$, haec enim expressio assumta est ad significandum, quot modis numerus n ex numeris 1 et 2 per additionem oriri possit. Hinc igitur erit:

$$\mathfrak{B}=1+1^{(2)}x+2^{(2)}x^2+3^{(2)}x^3+4^{(2)}x^4+5^{(2)}x^5+6^{(2)}x^6+\text{etc.}$$

atque ad similitudinem hujus expressionis erit:

$$\mathfrak{A}=1+1^{(1)}x+2^{(1)}x^2+3^{(1)}x^3+4^{(1)}x^4+5^{(1)}x^5+6^{(1)}x^6+\text{etc.}$$

Deinde vero cum sit $\mathfrak{A}=\frac{1}{1-x}$ et $\mathfrak{B}=\frac{1}{(1-x)(1-x^2)}$, erit $\mathfrak{A}=\mathfrak{B}(1-x^2)$, unde sequens inter has series relatio oritur:

$$\begin{aligned}\mathfrak{A} &= 1+1^{(1)}x+2^{(1)}x^2+3^{(1)}x^3+4^{(1)}x^4+5^{(1)}x^5+6^{(1)}x^6+\text{etc.}\\ \left.\begin{aligned}+\mathfrak{B}\\ -\mathfrak{B}x^2\end{aligned}\right\} &= \begin{aligned}1+1^{(2)}x+2^{(2)}x^2+3^{(2)}x^3+4^{(2)}x^4+5^{(2)}x^5+6^{(2)}x^6+\text{etc.}\\ -x^2-1^{(2)}x^3-2^{(2)}x^4-3^{(2)}x^5-4^{(2)}x^6-\text{etc.}\end{aligned}\end{aligned}$$

Quodsi hinc coaequatio terminorum homogeneorum instituatur, erit:

$1^{(2)} = 1^{(1)}$	$4^{(2)} = 4^{(1)} + 2^{(2)}$	$7^{(2)} = 7^{(1)} + 5^{(2)}$
$2^{(2)} = 2^{(1)} + 1$	$5^{(2)} = 5^{(1)} + 3^{(2)}$	$8^{(2)} = 8^{(1)} + 6^{(2)}$
$3^{(2)} = 3^{(1)} + 1^{(2)}$	$6^{(2)} = 6^{(1)} + 4^{(2)}$	$9^{(2)} = 9^{(1)} + 7^{(2)}$

§ 30. Generaliter ergo erit $n^{(2)} = n^{(1)} + (n-2)^{(2)}$. Cum igitur sit $n^{(1)} = 1$, erit

$$n^{(2)} = 1 + (n-2)^{(2)};$$

sicque coefficientes seriei $\mathfrak{B}$ ita determinabuntur, ut quisque terminus ultimus aequalis sit antepenultimo unitate aucto. Seu cum seriei $\mathfrak{A}$ omnes coefficientes sint unitates, ex serie $\mathfrak{A}$ sequenti modo series $\mathfrak{B}$ formabitur:

$$\begin{array}{l} \mathfrak{A} = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + \text{etc.} \\ \qquad\qquad\qquad 1 + 1 + 2 + 2 + 3 + 3 + 4 + 4 \\ \hline \mathfrak{B} = 1 + x + 2x^2 + 2x^3 + 3x^4 + 3x^5 + 4x^6 + 4x^7 + 5x^8 + 5x^9 + \text{etc.} \end{array}$$

Scilicet cum seriei $\mathfrak{B}$ duo termini initiales $1 + x$ constent, subscribantur ii sub terminis tertio et quarto seriei $\mathfrak{A}$, hincque per additionem orientur termini tertius et quartus seriei $\mathfrak{B}$, qui porro terminis quinto et sexto seriei $\mathfrak{A}$ subscripti et additi dabunt terminos quintum et sextum seriei $\mathfrak{B}$, hocque modo series $\mathfrak{B}$, quousque libuerit, facillime continuatur. Patet autem hinc esse

$n^{(2)} = \frac{1}{2}(n \pm \frac{1}{2})$, scilicet si n est numerus impar, erit
$n^{(2)} = \frac{1}{2}(n + 1)$, sin autem n sit numerus par, erit
$n^{(2)} = \frac{1}{2}(n + 2)$.

§ 31. Cum porro sit $\mathfrak{C} = \frac{1}{(1-x)(1-x^2)(1-x^3)}$, erit $\mathfrak{B} = \mathfrak{C}(1 - x^3)$, unde cum seriei $\mathfrak{C}$ terminus generalis sit $n^{(3)} x^n$, sequens nascetur relatio inter series $\mathfrak{B}$ et $\mathfrak{C}$:

$$\begin{array}{lll} \mathfrak{B} & = & 1 + 1^{(2)}x + 2^{(2)}x^2 + 3^{(2)}x^3 + 4^{(2)}x^4 + 5^{(2)}x^5 + 6^{(2)}x^6 + \text{etc.} \\ \left.\begin{array}{l} + \mathfrak{C} \\ - \mathfrak{C}x^3 \end{array}\right\} & = & \begin{array}{l} 1 + 1^{(3)}x + 2^{(3)}x^2 + 3^{(3)}x^3 + 4^{(3)}x^4 + 5^{(3)}x^5 + 6^{(3)}x^6 + \text{etc.} \\ \qquad\qquad\qquad - x^3 - 1^{(3)}x^4 - 2^{(3)}x^5 - 3^{(3)}x^6 - \text{etc.} \end{array} \end{array}$$

Si jam hic aequatio inter terminos homogeneos instituatur, erit:

$1^{(3)} = 1^{(2)}$	$4^{(3)} = 4^{(2)} + 1^{(3)}$	$7^{(3)} = 7^{(2)} + 4^{(3)}$
$2^{(3)} = 2^{(2)}$	$5^{(3)} = 5^{(2)} + 2^{(3)}$	$8^{(3)} = 8^{(2)} + 5^{(3)}$
$3^{(3)} = 3^{(2)} + 1$	$6^{(3)} = 6^{(2)} + 3^{(3)}$	$9^{(3)} = 9^{(2)} + 6^{(3)}$

et generaliter

$$n^{(3)} = n^{(2)} + (n-3)^{(3)}.$$

Series ergo $\mathfrak{C}$ ex serie $\mathfrak{B}$ suisque terminis antecedentibus sequenti modo facile formatur. Omittamus autem potestates ipsius x, quia totum negotium in coefficientibus versatur:

$$\begin{array}{l} \mathfrak{B} = 1 + 1 + 2 + 2 + 3 + 3 + 4 + 4 + 5 + 5 + 6 + 6 + \text{etc.} \\ \qquad\qquad\qquad\quad 1 + 1 + 2 + 3 + 4 + 5 + 7 + 8 + 10 \\ \hline \mathfrak{C} = 1 + 1 + 2 + 3 + 4 + 5 + 7 + 8 + 10 + 12 + 14 + 16 + \text{etc.} \end{array}$$

Scilicet seriei $\mathfrak{B}$ subscribatur series $\mathfrak{C}$, initium sub termino quarto faciendo, et prouti hoc modo series $\mathfrak{C}$ per additionem oritur, ita quoque sub serie $\mathfrak{B}$ continuabitur.

§ 32. Quia deinde est $\mathfrak{D} = \frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)}$, erit $\mathfrak{C} = (1-x^4)\,\mathfrak{D}$. Unde simili modo, quo hactenus sumus usi, reperietur:

$1^{(4)} = 1^{(3)}$	$4^{(4)} = 4^{(3)} + 1$	$7^{(4)} = 7^{(3)} + 3^{(4)}$
$2^{(4)} = 2^{(3)}$	$5^{(4)} = 5^{(3)} + 1^{(4)}$	$8^{(4)} = 8^{(3)} + 4^{(4)}$
$3^{(4)} = 3^{(3)}$	$6^{(4)} = 6^{(3)} + 2^{(4)}$	$9^{(4)} = 9^{(3)} + 5^{(4)}$

et generaliter

$$n^{(4)} = n^{(3)} + (n-4)^{(4)}.$$

Pari modo ulterius progrediendo colligetur fore:

$$n^{(5)} = n^{(4)} + (n-5)^{(5)}$$
$$n^{(6)} = n^{(5)} + (n-6)^{(6)}$$
$$n^{(7)} = n^{(6)} + (n-7)^{(7)}$$
etc.

Generatim ergo hinc colligetur fore:

$$n^{(m)} = n^{(m-1)} + (n-m)^{(m)}.$$

Ubi notandum est, si fuerit $n < m$, tum terminum $(n-m)^{(m)}$ prorsus evanescere, sin autem sit $n = m$, etiamsi sit $n - m = 0$, tamen terminum $(n-m)^{(m)}$ valere unitatem. Deinde si sit $n - m = 1$, quoque erit $(n-m)^{(m)} = 1$. Erit ergo perpetuo tam $0^{(m)} = 1$, quam $1^{(m)} = 1$ et $n^{(1)} = 1$.

§ 33. His relationibus inter series $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc. notatis, eae facillime formantur, et quousque libuerit, continuantur, quae operatio per hic adjunctum schematismum fiet manifestum:

	1	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}	x^{14}	x^{15}	etc.
𝔄 =	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	etc.
			1	1	2	2	3	3	4	4	5	5	6	6	7	7	etc.
𝔅 =	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	etc.
				1	1	2	3	4	5	7	8	10	12	14	16	19	etc.
ℭ =	1	1	2	3	4	5	7	8	10	12	14	16	19	21	24	27	etc.
					1	1	2	3	5	6	9	11	15	18	23	27	etc.
𝔇 =	1	1	2	3	5	6	9	11	15	18	23	27	34	39	47	54	etc.
						1	1	2	3	5	7	10	13	18	23	30	etc.
𝔈 =	1	1	2	3	5	7	10	13	18	23	30	37	47	57	70	84	etc.
							1	1	2	3	5	7	11	14	20	26	etc.
𝔉 =	1	1	2	3	5	7	11	14	20	26	35	44	58	71	90	110	etc.
								1	1	2	3	5	7	11	15	21	etc.
𝔊 =	1	1	2	3	5	7	11	15	21	28	38	49	65	82	105	131	etc.
									1	1	2	3	5	7	11	15	etc.
ℌ =	1	1	2	3	5	7	11	15	22	29	40	52	70	89	116	146	etc.
										1	1	2	3	5	7	11	etc.
ℑ =	1	1	2	3	5	7	11	15	22	30	41	54	73	94	123	157	etc.
											1	1	2	3	5	7	etc.
𝔎 =	1	1	2	3	5	7	11	15	22	30	42	55	75	97	128	164	etc.
												1	1	2	3	5	etc.
𝔏 =	1	1	2	3	5	7	11	15	22	30	42	56	76	99	131	169	etc.
													1	1	2	3	etc.
𝔐 =	1	1	2	3	5	7	11	15	22	30	42	56	77	100	133	172	etc.
														1	1	2	etc.
𝔑 =	1	1	2	3	5	7	11	15	22	30	42	56	77	101	134	174	etc.

§ 34. Hoc modo tabula hic adjuncta per solam continuam additionem est constructa, atque ratio constructionis tam est perspicua ex inspectione, ut ampliore explicatione non egeat. Ope hujus tabulae igitur immediate resolvitur hoc problema, quo quaeritur, *quot variis modis datus numerus* n *ex his numeris* 1, 2, 3,........m *per additionem produci possit.*

Sic si quaeratur, quot variis modis numerus 10 ex his numeris 1, 2, et 3 per additionem oriri possit, erit $n = 10$ et $m = 3$, atque ex tabula reperitur modorum numerus $= 14$, qui modi sunt:

$10 = 1+1+1+1+1+1+1+1+1+1$	$10 = 1+1+1+2+2+3$
$10 = 1+1+1+1+1+1+1+1+2$	$10 = 1+1+2+2+2+2$
$10 = 1+1+1+1+1+1+1+3$	$10 = 1+1+2+3+3$
$10 = 1+1+1+1+1+1+2+2$	$10 = 1+2+2+2+3$
$10 = 1+1+1+1+1+2+3$	$10 = 1+3+3+3$
$10 = 1+1+1+1+2+2+2$	$10 = 2+2+2+2+2$
$10 = 1+1+1+1+3+3$	$10 = 2+2+3+3$

Si quaeratur, quot variis modis numerus 25 ex his numeris 1, 2, 3, 4, 5 per additionem produci possit, facto $n = 25$ et $m = 5$, reperietur ex tabula numerus modorum $= 377$.

Si quaeratur quot variis modis numerus 50 ex his numeris 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 per additionem resultare possit, posito $n = 50$ et $m = 10$, invenitur modorum numerus $= 62740$.

Si vel numerus propositus, vel numerus partium major sit quam in tabula, tum nihilo minus casuum numerus ex tabula ope formularum supra inventarum colligi poterit. Uti si quaeratur, quot modis numerus 60 ex his numeris 1, 2, 3.....20 per additionem resultare possit, erit $n = 60$ et $m = 20$, quaeriturque valor formulae $60^{(20)}$. Est vero $60^{(20)} = 60^{(19)} + 40^{(20)}$, at $60^{(19)} = 60^{(18)} + 41^{(19)}$, porroque $60^{(18)} = 60^{(17)} + 42^{(18)}$, et $60^{(17)} = 60^{(16)} + 43^{(17)}$, sicque deinceps. Unde tandem erit

$$60^{(20)} = 40^{(20)} + 41^{(19)} + 42^{(18)} + 43^{(17)} + 44^{(16)} + \dots\dots + 59^{(1)},$$

qui numeri ex tabula collecti dant 791131, totque modis numerus 60 ex numeris 1, 2, 3......20 per additionem elici potest.

§ 35. Ope hujus tabulae deinde ambo problemata cel. Naudei expedite resolvi possunt. Ac primo quidem si quaeratur, *quot variis modis datus numerus* N *in* m *partes inter se inaequales dispertiri possit, hoc fiet, uti supra ostendimus, tot modis, quot unitates continentur in hac expressione* $\left(N - \frac{m(m+1)}{2}\right)^{(m)}$ *quam tabula indicat.*

Usum igitur hujus tabulae aliquot exemplis ostendamus.

I. *Quaeratur, quot variis modis numerus 25 in quinque partes inaequales dispertiri possit?*

Erit ergo hic $N = 25$ et $m = 5$, unde $\frac{m(m+1)}{2} = 15$ et responsum continebit formula $10^{(5)}$, quae ex tabula est $= 30$, ita ut partitio 30 modis institui possit.

II. *Quaeratur, quot variis modis numerus 50 in 7 partes inaequales dispertiri possit?*

Hic est $N = 50$, $m = 7$ et $N - \frac{m(m+1)}{2} = 22$, unde numerus partitionum quaesitus est $= 22^{(7)} = 522$.

III. *Quaeratur, quot variis modis numerus 100 in 10 partes inaequales dispertiri possit?*

Cum sit $N = 100$ et $m = 10$, erit $N - \frac{m(m+1)}{2} = 45$ et numerus partitionum reperietur $45^{(10)} = 33401$.

IV. *Quaeratur, quot diversis modis numerus 256 in 20 partes inaequales dispertiri possit?*

Ob $N = 256$ et $m = 20$, erit $N - \frac{m(m+1)}{2} = 46$, et numerus partitionum fiet $= 46^{(20)} = 96271$.

V. *Quaeratur, quot diversis modis numerus 270 in 20 partes inaequales dispertiri possit?*

Ob $N = 270$ et $m = 20$, erit $N - \frac{m(m+1)}{2} = 60$, ideoque numerus partitionum quaesitus fit $= 60^{(20)}$, cujus valorem ante invenimus esse $= 791131$. Tot ergo diversis modis numerus 270 in 20 partes inaequales dispertiri potest.

§ 36. Simili modo ex tabula quoque alterum problema resolvetur, quo quaerebatur: *quot variis modis numerus N in m partes aequalitate partium non exclusa dispertiri possit?*

Supra enim ostendimus partitionum numerum quaesitum contineri in hac formula $(N-m)^{(m)}$, quem valorem ex tabula depromere licet. Quae solutio quo facilius intelligatur, aliquot exempla adjiciamus.

I. *Quaeratur, quot variis modis numerus 25 in quinque partes sive aequales, sive inaequales dispertiri possit?*

Hic est $N = 25$ et $m = 5$, unde $N - m = 20$, et partitionum numerus erit $20^{(5)} = 192$.

II. *Quaeratur, quot variis modis numerus 50 in septem partes sive aequales, sive inaequales dispertiri possit?*

Ob $N = 50$ et $m = 7$, erit $N - m = 43$; et partitionum numerus quaesitus fiet $43^{(7)} = 8946$.

III. *Quaeratur, quot variis modis numerus 50 in decem partes sive aequales, sive inaequales dispertiri possit?*

Ob $N = 50$ et $m = 10$, erit $N - m = 40$ et partitionum numerus erit $40^{(10)} = 16928$.

IV. *Quaeratur, quot variis modis numerus 60 in 12 partes sive aequales, sive inaequales dispertiri possit?*

Cum sit $N = 60$ et $m = 12$, erit $N - m = 48$, et partitionum numerus quaesitus erit $48^{(12)} = 74287$.

V. *Quaeratur, quot variis modis numerus 80 in 20 partes sive aequales, sive inaequales dispertiri possit?*

Erit ergo $N = 80$ et $m = 20$, unde $N - m = 60$, et partitionum numerus erit

$$= 60^{(20)} = 791131.$$

§ 37. In seriebus horizontalibus, quas tabula exhibet, notatu digna est convenientia inter terminos initiales harum serierum, quae eo longius procedit, quo major fuerit numerus m: sic series decima quinta quindecim suos terminos initiales cum omnibus seriebus sequentibus habet communes. Hinc inveniri poterit series, quae numero m in infinitum aucto respondet, quae ergo continebit valores hujus formulae $n^{(\infty)}$, quae denotat, quot variis modis numerus n, ex omnibus prorsus numeris integris per additionem produci possit. Haec ergo quaestio digna videtur, quae diligentius evolvatur. Cum $n^{(\infty)}$ complectatur omnes omnino partitiones numeri n, pro quocunque partium numero simul sumtas: erit $n^{(\infty)}$ aggregatum ex numeris partitionum in 1, 2, 3, 4, ... usque ad n partes, sive aequales, sive inaequales: quia numerus n in plures quam n partes secari nequit. Quamobrem erit:

$$n^{(\infty)} = (n-1)^{(1)} + (n-2)^{(2)} + (n-3)^{(3)} + (n-4)^{(4)} + (n-5)^{(5)} + \ldots\ldots + (n-n)^{(n)}$$

in qua serie tam primus terminus $(n-1)^{(1)}$, qui denotat sectionem in unam partem, quam ultimus $(n-n)^{(n)}$, qui denotat sectionem in n partes, est unitas. Hinc igitur series numerorum $n^{(\infty)}$,

quae in calce tabulae exhibetur per additionem terminorum, ex superioribus seriebus inveniri potest. Sic erit:

$$6^{(\infty)} = 5^{(1)} + 4^{(2)} + 3^{(3)} + 2^{(4)} + 1^{(5)} + 0^{(6)} = 1 + 3 + 3 + 2 + 1 + 1 = 11,$$

qui numerus in infima tabulae serie sub numero 6 habetur.

§ 38. Potest autem haec operatio contrahi ope lemmatis supra inventi

$$n^{(m)} = n^{(m-1)} + (n-m)^{(m)},$$

unde fit

$$n^{(m)} - n^{(m-1)} = (n-m)^{(m)}.$$

Cum enim sit:

$$n^{(\infty)} = (n-1)^{(1)} + (n-2)^{(2)} + (n-3)^{(3)} + (n-4)^{(4)} + (n-5)^{(5)} + (n-6)^{(6)} + \text{etc.}$$

si ubique loco n scribatur $n-1$, erit:

$$(n-1)^{(\infty)} = (n-1)^{(0)} + (n-2)^{(1)} + (n-3)^{(2)} + (n-4)^{(3)} + (n-5)^{(4)} + (n-6)^{(5)} + \text{etc.}$$

ubi ob uniformitatem praefigitur terminus $(n-1)^{(0)}$, cujus valor est $= 0$. Si igitur inferior series a superiori subtrahatur, ope lemmatis prodibit:

$$n^{(\infty)} - (n-1)^{(\infty)} = (n-2)^{(1)} + (n-4)^{(2)} + (n-6)^{(3)} + (n-8)^{(4)} + (n-10)^{(5)} + (n-12)^{(6)} + \text{etc.}$$

sicque terminus quisque $n^{(\infty)}$ ope praecedentis $(n-1)^{(\infty)}$ per additionem duplo pauciorum terminorum quam ante invenitur. Erit ergo ex: gr.:

$$12^{(\infty)} = 11^{(\infty)} + 10^{(1)} + 8^{(2)} + 6^{(3)} + 4^{(4)} + 2^{(5)} + 0^{(6)}$$

sive

$$12^{(\infty)} = 56 + 1 + 5 + 7 + 5 + 2 + 1 = 77,$$

qui numerus quoque pro valore ipsius $12^{(\infty)}$ in tabula reperitur.

§ 39. Simili modo haec operatio ulterius contrahi potest, cum enim sit:

$$n^{(\infty)} - (n-1)^{(\infty)} = (n-2)^{(1)} + (n-4)^{(2)} + (n-6)^{(3)} + (n-8)^{(4)} + (n-10)^{(5)} + \text{etc.}$$

si loco n ponamus $n-2$, habebimus:

$$(n-2)^{(\infty)} - (n-3)^{(\infty)} = (n-2)^{(0)} + (n-4)^{(1)} + (n-6)^{(2)} + (n-8)^{(3)} + (n-10)^{(4)} + \text{etc.}$$

ubi ob uniformitatem terminum $(n-2)^{(0)} = 0$ praemittimus. Nunc hanc seriem a superiore subtrahendo ope lemmatis obtinebimus

$$\left.\begin{array}{l} + n^{(\infty)} - (n-1)^{(\infty)} \\ - (n-2)^{(\infty)} + (n-3)^{(\infty)} \end{array}\right\} = (n-3)^{(1)} + (n-6)^{(2)} + (n-9)^{(3)} + (n-12)^{(4)} + (n-15)^{(5)} + \text{etc.}$$

Haec ergo series si dicatur $= P$, erit:

$$n^{(\infty)} = (n-1)^{(\infty)} + (n-2)^{(\infty)} - (n-3)^{(\infty)} + P.$$

In serie ergo quaesita ad definiendum terminum quemvis $n^{(\infty)}$, praeter valorem ipsius P nosse oportet ternos terminos praecedentes. Hoc modo procedendo tandem quantitas P evanescet, et quilibet terminus istius seriei per solos terminos praecedentes definietur, quae est proprietas serierum recurrentium.

§ 40. Hanc vero seriem re vera esse recurrentem ex ejus genesi est manifestum, cum oriatur ex evolutione hujus fractionis:

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)\text{ etc.}}.$$

Scala ergo relationis istius seriei habebitur, si iste denominator actu per multiplicationem evolvatur. Instituta autem hac multiplicatione denominator sequenti modo expressus invenietur:

$$1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+x^{51}+x^{57}-x^{70}-x^{77}+\text{ etc.}$$

Quae ipsius x potestates qualem teneant legem, ex ipsa formatione vix definiri posse videtur; interim tamen ex inspectione mox patet, alternatim binos terminos esse affirmativos et negativos. Neque minus exponentes ipsius x certam legem tenere observantur, unde ejus terminus generalis colligitur esse

$$x^{\frac{n(3n\pm1)}{2}}.$$

Scilicet nullae aliae potestates occurrunt, nisi quarum exponentes continentur in hac formula $\frac{3nn\pm n}{2}$, et ita quidem ut potestates, quae ex numeris imparibus pro n assumtis oriuntur, habeant signum $-$, quae vero ex numeris paribus formantur, signum $+$.

§ 41. Haec igitur forma nobis suppeditat scalam relationis seriei quaesitae, quam constat fore:

$$n^{(\infty)}=(n-1)^{(\infty)}+(n-2)^{(\infty)}-(n-5)^{(\infty)}-(n-7)^{(\infty)}+(n-12)^{(\infty)}+(n-15)^{(\infty)}-(n-22)^{(\infty)}$$
$$-(n-26)^{(\infty)}+(n-35)^{(\infty)}+(n-40)^{(\infty)}-(n-51)^{(\infty)}-(n-57)^{(\infty)}+\text{ etc.}$$

Hanc autem legem progressionis locum haberi tentanti facile patebit. Sit enim $n=30$ reperietur fore:

$$30^{(\infty)}=29^{(\infty)}+28^{(\infty)}-25^{(\infty)}-23^{(\infty)}+18^{(\infty)}+15^{(\infty)}-8^{(\infty)}-4^{(\infty)}$$

est enim his numeris ex tabula desumtis

$$5604=4565+3718-1958-1255+385+176-22-5.$$

Atque hoc modo ista series quousque libuerit continuari potest.

§ 42. Quoniam vero series pro valore $m=20$ jam est formata, ex ea aliquanto facilius series quaesita pro valore $m=\infty$ erui poterit. Cum enim series $n^{(20)}$ formetur ex evolutione hujus fractionis:

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\ldots\ldots(1-x^{20})}$$

series vero $n^{(\infty)}$ ex evolutione hujus fractionis:

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)\ldots\ldots(1-x^{(\infty)})}$$

manifestum est si haec series multiplicetur per

$$(1-x^{21})(1-x^{22})(1-x^{23})(1-x^{24})(1-x^{25})\text{ etc.}$$

seu per

$$1-x^{21}-x^{22}-x^{23}-x^{24}-x^{25}-x^{26}-x^{27}-\text{ etc.}$$
$$+x^{43}+x^{44}+2x^{45}+2x^{46}+3x^{47}+3x^{48}+4x^{49}+4x^{50}+\text{ etc.}$$
$$-x^{66}-x^{67}-2x^{68}-3x^{69}-4x^{70}-5x^{71}-7x^{72}-8x^{73}-10x^{74}-\text{ etc.}$$
$$+x^{90}+x^{91}+2x^{92}+3x^{93}+5x^{94}+6x^{95}+9x^{96}+11x^{97}+15x^{98}+\text{ etc.}$$
$$-x^{115}-x^{116}-2x^{117}-3x^{118}-5x^{119}-7x^{120}-10x^{121}-13x^{122}-18x^{123}-\text{ etc.}$$

etc.

tum prodire debere priorem. Hinc concluditur fore:

$$\begin{aligned} n^{(20)} = \; & n^{(\infty)} - (n-21)^{(\infty)} - (n-22)^{(\infty)} - (n-23)^{(\infty)} - (n-24)^{(\infty)} - \text{etc.} \\ & + (n-43)^{(\infty)} + (n-44)^{(\infty)} + 2(n-45)^{(\infty)} + 2(n-46)^{(\infty)} + 3(n-47)^{(\infty)} + \text{etc.} \\ & - (n-66)^{(\infty)} - (n-67)^{(\infty)} - 2(n-68)^{(\infty)} - 3(n-69)^{(\infty)} - 4(n-70)^{(\infty)} - \text{etc.} \\ & + (n-90)^{(\infty)} + (n-91)^{(\infty)} + 2(n-92)^{(\infty)} + 3(n-93)^{(\infty)} + 5(n-94)^{(\infty)} + \text{etc.} \\ & - (n-115)^{(\infty)} - (n-116)^{(\infty)} - 2(n-117)^{(\infty)} - 3(n-118)^{(\infty)} - 5(n-119)^{(\infty)} - \text{etc.} \\ & \text{etc.} \end{aligned}$$

quarum serierum coefficientes procedunt secundum series superiores pro partitione numerorum in 2, 3, 4, 5, 6, etc. partes inservientes.

§ 43. Denotet $f(n-21)^{(\infty)}$ summam omnium terminorum seriei $n^{(\infty)}$, quae est:

$$1 + 1 + 2 + 3 + 5 + 7 + 11 + 15 + 22 + 30 + \text{etc.}$$

usque ad terminum $(n-21)^{(\infty)}$ inclusive: similique modo sit generaliter $fp^{(\infty)}$ summa omnium terminorum ejusdem seriei usque ad terminum $p^{(\infty)}$ inclusive, quae summae cum successive facile formentur, erit

$$\begin{aligned} n^{(20)} = n^{(\infty)} & - f(n-21)^{(\infty)} + f(n-43)^{(\infty)} + f(n-45)^{(\infty)} + f(n-47)^{(\infty)} + \text{etc.} \\ & - f(n-66)^{(\infty)} - f(n-68)^{(\infty)} - f(n-69)^{(\infty)} - f(n-70)^{(\infty)} - \text{etc.} \\ & + f(n-90)^{(\infty)} + f(n-92)^{(\infty)} + f(n-93)^{(\infty)} + f(n-94)^{(\infty)} + \text{etc.} \\ & \text{etc.} \end{aligned}$$

Hincque adeo erit:

$$\begin{aligned} n^{(\infty)} = n^{(20)} & + f(n-21)^{(\infty)} - f(n-43)^{(\infty)} - f(n-45)^{(\infty)} - f(n-47)^{(\infty)} - \text{etc.} \\ & + f(n-66)^{(\infty)} + f(n-68)^{(\infty)} + f(n-69)^{(\infty)} + f(n-70)^{(\infty)} + \text{etc.} \\ & - f(n-90)^{(\infty)} - f(n-92)^{(\infty)} - f(n-93)^{(\infty)} - f(n-94)^{(\infty)} - \text{etc.} \\ & \text{etc.} \end{aligned}$$

Hujus formulae ope, nisi n sit numerus valde magnus, ex serie pro partitione in 20 partes inserviente ipsa series $n^{(\infty)}$ facile constituitur, hocque modo ea in tabula constructa exhibetur, cum ubique excessus terminorum $n^{(\infty)}$ supra terminos $n^{(20)}$ sint assignati.

§ 44. Hac igitur serie constructa, proposito quocunque numero definiri poterit, quot omnino modis is in partes dispertiri possit. Sic patet numerum 10 omnino 42 modis ex additione resultare posse; atque numerus 59 tot modis, quot indicat iste numerus 831820 per additionem produci poterit. Sin autem numeri majores proponantur, tum tabula hic exhibita ulterius continuari, vel pro quovis casu numerus desideratus per praecepta hic tradita investigari debet. In his autem partitionibus aequalitas partium non excluditur. Unde novum oritur problema, *quo pro quovis numero proposito quaeritur omnium partitionum numerus in partes inter se inaequales*, quod problema resolvetur ope hujus expressionis:

$$(1+x)(1+x^2)(1+x^3)(1+x^4)(1+x^5)(1+x^6) \text{ etc.}$$

His enim factoribus in se invicem multiplicatis orietur series, in qua quilibet coefficiens ostendet, quot variis modis exponens ipsius x in partes inter se inaequales dispertiri possit.

§ 45. Quod si autem hoc productum actu evolvatur, reperietur haec series:

$$1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + 4x^6 + 5x^7 + 6x^8 + 8x^9 + 10x^{10} + 12x^{11} + 15x^{12} + 18x^{13} + 22x^{14} + 27x^{15} + 32x^{16} + 38x^{17} + 46x^{18} + 54x^{19} + 64x^{20} + 76x^{21} + 89x^{22} + \text{etc.}$$

quae cum sit productum ex factoribus infinitis tam simplicem legem servantibus, omni attentione digna videtur. Ac primo quidem manifestum est coefficientes horum terminorum plerumque esse pares, et eos solum esse impares, qui sint cum ejusmodi ipsius x potestatibus conjuncti, quarum exponentes in hac forma $\frac{3nn \pm n}{2}$ contineantur: cujus phaenomeni eadem est ratio, atque illius, quod circa exponentes ejusdem formae $\frac{3nn \pm n}{2}$ in evolutione producti

$$(1 - x)(1 - x^2)(1 - x^3)(1 - x^4) \text{ etc.}$$

observavimus. Cum autem sit:

$$(1 + x)(1 + x^2)(1 + x^3)(1 + x^4) \text{ etc.} = \frac{(1 - x^2)(1 - x^4)(1 - x^6)(1 - x^8) \text{ etc.}}{(1 - x)(1 - x^2)(1 - x^3)(1 - x^4) \text{ etc.}}$$

apparet, seriem ante inventam exprimi hac fractione:

$$\frac{1 - x^2 - x^4 + x^{10} + x^{14} - x^{24} - x^{30} + x^{44} + x^{52} - x^{70} - x^{80} + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \text{etc.}},$$

unde ea ad modum serierum recurrentium formari poterit.

§ 46. Facillime autem sine dubio haec series construitur ex ipsa ejus indole, qua cujuslibet termini coefficiens indicare debet, quot variis modis exponens ipsius x in partes inaequales dispertiri possit. Sit N coefficiens potestatis x^n in ista serie, eritque:

$$N = (n - 1)^{(1)} + (n - 3)^{(2)} + (n - 6)^{(3)} + (n - 10)^{(4)} + (n - 15)^{(5)} + (n - 21)^{(6)} + \text{etc.}$$

nam $(n - 1)^{(1)} = 1$ indicat numerum n unico modo ex una parte constare: $(n - 3)^{(2)}$ ostendit, quot modis numerus n in duas partes inaequales, $(n - 6)^{(3)}$ ostendit, quot modis numerus n in tres partes inaequales distribui possit, et ita porro: unde et haec series ope tabulae datae quousque libuerit continuari potest. Ceterum hic notatu dignum est, si numeri partitionum in partes numero pares negative capiantur, hanc expressionem resultantem:

$$(n - 1)^{(1)} - (n - 3)^{(2)} + (n - 6)^{(3)} - (n - 10)^{(4)} + (n - 15)^{(5)} - (n - 21)^{(6)} + \text{etc.}$$

semper esse $= 0$, nisi fuerit n numerus in hac forma contentus $\frac{3zz \pm z}{2}$; sin autem n in hac forma contineatur, tum illius expressionis valorem esse vel $+1$ vel -1, prout z fuerit numerus vel impar vel par.

§ 47. Quemadmodum hactenus omnes numeros integros ad partes constituendas admisimus, ita partium conditione limitanda numerus quaestionum in infinitum augeri posset: cui negotio, cum methodus certa ad hujusmodi quaestiones resolvendas sit tradita, non diutius immorabimur. Sufficiat ex praecedente insignem proprietatem partitionis in partes impares annotasse. Cum sit:

$$(1 + x)(1 + x^2)(1 + x^3)(1 + x^4) \text{ etc.} = \frac{1}{(1 - x)(1 - x^3)(1 - x^5)(1 - x^7)(1 - x^9) \text{ etc.}}$$

quae formula ex aequatione in § 44 exhibita sponte fluit, hinc sequitur, quemvis numerum totidem

modis ex numeris solis imparibus per additionem produci posse, quot modis idem numerus omnino in partes inter se inaequales dispertiri possit. Sic cum numerus 10 decem modis in partes inaequales dispertiri possit, qui modi sunt:

$10 = 10$	$10 = 1 + 2 + 7$
$10 = 1 + 9$	$10 = 1 + 3 + 6$
$10 = 2 + 8$	$10 = 1 + 4 + 5$
$10 = 3 + 7$	$10 = 2 + 3 + 5$
$10 = 4 + 6$	$10 = 1 + 2 + 3 + 4$

idem numerus 10 quoque decem modis ex solis numeris imparibus per additionem produci potest, hoc modo

$10 = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$	$10 = 1 + 3 + 3 + 3$
$10 = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 3$	$10 = 1 + 1 + 1 + 1 + 3 + 3$
$10 = 1 + 1 + 1 + 1 + 1 + 5$	$10 = 1 + 1 + 3 + 5$
$10 = 1 + 1 + 1 + 7$	$10 = 3 + 7$
$10 = 1 + 9$	$10 = 5 + 5$

§ 48. Relictis autem his speculationibus progredior ad investigandum, quomodo quisque numerus ex terminis progressionis geometricae 1, 2, 4, 8, 16, 32, etc. per additionem formari possit. Ac primo quidem si istae partes inter se debeant esse omnes inaequales, quaestio resolvetur per evolutionem hujus expressionis:

$$s = (1 + x)(1 + x^2)(1 + x^4)(1 + x^8)(1 + x^{16})(1 + x^{32}) \text{ etc.}$$

Multiplicatione enim actu instituta, cujusque termini coefficiens indicabit, quot modis exponens potestatis ipsius x adjunctae ex numeris progressionis geometricae 1, 2, 4, 8, 16, etc. per additionem produci possit. Cum igitur quivis numerus unico modo sic resolvi posse observatus sit, ostendendum est in hac serie omnes ipsius x potestates occurrere, omniumque eundem esse coefficientem unitatem.

§ 49. Ut hoc demonstremus, ponamus esse

$$s = 1 + \alpha x + \beta x^2 + \gamma x^3 + \delta x^4 + \varepsilon x^5 + \zeta x^6 + \eta x^7 + \vartheta x^8 + \text{etc.}$$

atque ad valores coefficientium α, β, γ, δ, etc. eruendos, ponamus xx loco x, sitque valor pro s hoc modo resultans $= t$, erit:

$$t = (1 + x^2)(1 + x^4)(1 + x^8)(1 + x^{16})(1 + x^{32}) \text{ etc.}$$

ideoque fiet $s = (1 + x)t$. Qua relatione in seriebus considerata, ob

$$t = 1 + \alpha x^2 + \beta x^4 + \gamma x^6 + \delta x^8 + \varepsilon x^{10} + \text{etc.}$$

habebitur:

$$(1 + x)t = 1 + x + \alpha x^2 + \alpha x^3 + \beta x^4 + \beta x^5 + \gamma x^6 + \gamma x^7 + \delta x^8 + \delta x^9 + \text{etc.}$$

quae cum aequalis esse debeat seriei s, comparatio coefficientium dabit:

$\alpha = 1$	$\delta = \beta$	$\eta = \gamma$	$\varkappa = \varepsilon$
$\beta = \alpha$	$\varepsilon = \beta$	$\vartheta = \delta$	$\lambda = \varepsilon$
$\gamma = \alpha$	$\zeta = \gamma$	$\iota = \delta$	$\mu = \zeta$ etc.

unde manifestum est, singulos coefficientes esse unitati aequales, ac propterea esse:

$$s = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + \text{etc.} = \frac{1}{1-x},$$

quod idem per se perspicuum est, cum sit:

$$(1-x)(1+x)(1+x^2)(1+x^4)(1+x^8)(1+x^{16}) \text{ etc.} = 1.$$

§ 50. Sin autem quaeratur, quot variis modis quisque numerus ex terminis progressionis geometricae 1, 2, 4, 8, 16, etc. partium aequalitate non amplius sublata, per additionem produci queat: solutio petenda erit ex evolutione hujus fractionis:

$$s = \frac{1}{(1-x)(1-x^2)(1-x^4)(1-x^8)(1-x^{16})(1-x^{32}) \text{ etc.}}$$

hac enim in serie evoluta, coefficiens cujusque termini ostendet, quot variis modis exponens potestatis ipsius x adjunctae ex terminis progressionis geometricae propositae per additionem resultare possit. Ponamus xx loco x, et valor ipsius s abeat in t, erit:

$$t = \frac{1}{(1-x^2)(1-x^4)(1-x^8)(1-x^{16}) \text{ etc.}} = (1-x)s.$$

Sit igitur

$$s = 1 + \alpha x + \beta x^2 + \gamma x^3 + \delta x^4 + \varepsilon x^5 + \zeta x^6 + \eta x^7 + \vartheta x^8 + \iota x^9 + \text{ etc.}$$

erit

$$\begin{aligned}(1-x)s &= 1 + \alpha x + \beta x^2 + \gamma x^3 + \delta x^4 + \varepsilon x^5 + \zeta x^6 + \eta x^7 + \vartheta x^8 + \iota x^9 + \text{ etc.}\\ &\quad - 1 - \alpha - \beta - \gamma - \delta - \varepsilon - \zeta - \eta - \vartheta - \text{etc.}\\ = t &= 1 \quad + \alpha x^2 \quad + \beta x^4 \quad + \gamma x^6 \quad + \delta x^8 \quad + \text{ etc.}\end{aligned}$$

unde ex aequalitate terminorum homogeneorum obtinebitur:

$\alpha = 1 \qquad = 1$	$\eta = \zeta \qquad = 6$	$\nu = \mu \qquad = 20$
$\beta = \alpha + \alpha = 2$	$\vartheta = \eta + \delta = 10$	$\xi = \nu + \eta = 26$
$\gamma = \beta \qquad = 2$	$\iota = \vartheta \qquad = 10$	$o = \xi \qquad = 26$
$\delta = \gamma + \beta = 4$	$\varkappa = \iota + \varepsilon = 14$	$\pi = o + \vartheta = 36$
$\varepsilon = \delta \qquad = 4$	$\lambda = \varkappa \qquad = 14$	$\varrho = \pi \qquad = 36$
$\zeta = \varepsilon + \gamma = 6$	$\mu = \lambda + \zeta = 20$	$\sigma = \varrho + \iota = 46$ etc.

§ 51. Notatu digna est haec series, cum quod bini termini sint ubique aequales, tum quod ea facillime quousque libuerit continuetur. Ulterius autem continuata ita se habebit:

$$\begin{aligned}&1 + x + 2x^2 + 2x^3 + 4x^4 + 4x^5 + 6x^6 + 6x^7 + 10x^8 + 10x^9 + 14x^{10} + 14x^{11} + 20x^{12} + 20x^{13}\\ &+ 26x^{14} + 26x^{15} + 36x^{16} + 36x^{17} + 46x^{18} + 46x^{19} + 60x^{20} + 60x^{21} + 74x^{22} + 74x^{23} + 94x^{24}\\ &+ 94x^{25} + 114x^{26} + 114x^{27} + 140x^{28} + 140x^{29} + 166x^{30} + 166x^{31} + 202x^{32} + 202x^{33}\\ &+ 238x^{34} + 238x^{35} + 284x^{36} + 284x^{37} + \text{ etc.}\end{aligned}$$

Ex hac ergo serie patet numerum verbi gratia 30 centum sexaginta et sex modis ex terminis pro-

gressionis geometricae duplae per additionem produci posse. Ceterum attendenti facile patebit, legem hujus progressionis nullo modo per terminum generalem exprimi posse, cum revera sit series recurrens, cujus scala relationis in infinitum extendatur. Dabit autem hoc productum infinitum:

$$(1-x)(1-x^2)(1-x^4)(1-x^8)(1-x^{16})(1-x^{32}) \text{ etc.}$$

si evolvatur, scalam relationis. Ad quam inveniendam ponatur hoc productum $= p$, quod abeat in q si loco x ponatur x^2, eritque:

$$q = (1-x^2)(1-x^4)(1-x^8)(1-x^{16}) \text{ etc.} = \frac{p}{1-x}, \quad \text{seu} \quad p = (1-x)\,q.$$

Statuatur ergo:

$$p = 1 + \alpha x + \beta x^2 + \gamma x^3 + \delta x^4 + \varepsilon x^5 + \zeta x^6 + \eta x^7 + \vartheta x^8 + \iota x^9 + \varkappa x^{10} + \text{etc.}$$

eritque:

$$(1-x)\,q = 1 - x + \alpha x^2 - \alpha x^3 + \beta x^4 - \beta x^5 + \gamma x^6 - \gamma x^7 + \delta x^8 - \delta x^9 + \varepsilon x^{10} - \text{etc.}$$

unde per coaequationem terminorum similium obtinetur:

$\alpha = -1 = -1$	$\vartheta = \delta = -1$	$o = -\eta = +1$	
$\beta = \alpha = -1$	$\iota = -\delta = +1$	$\pi = \vartheta = -1$	
$\gamma = -\alpha = +1$	$\varkappa = \varepsilon = +1$	$\varrho = -\vartheta = +1$	
$\delta = \beta = -1$	$\lambda = -\varepsilon = -1$	$\sigma = \iota = +1$	
$\varepsilon = -\beta = +1$	$\mu = \zeta = +1$	$\tau = -\iota = -1$	
$\zeta = \gamma = +1$	$\nu = -\zeta = -1$	$\upsilon = \varkappa = +1$	
$\eta = -\gamma = -1$	$\xi = \eta = -1$	$\varphi = -\varkappa = -1$	etc.

§ 52. Coefficientes ergo seriei p, quae ex evolutione hujus producti:

$$(1-x)(1-x^2)(1-x^4)(1-x^8)(1-x^{16})(1-x^{32}) \text{ etc.}$$

nascitur, omnes sunt vel $+1$ vel -1, neque tamen legem obtinent solito more assignabilem, erit enim:

$$p = 1 - x^1 - x^2 + x^3 - x^4 + x^5 + x^6 - x^7 - x^8 + x^9 + x^{10} - x^{11} + x^{12} - x^{13} - x^{14} + x^{15}$$
$$- x^{16} + x^{17} + x^{18} - x^{19} + x^{20} - x^{21} - x^{22} + x^{23} + x^{24} - x^{25} - x^{26} + x^{27} - x^{28} + x^{29} + x^{30}$$
$$- x^{31} - x^{32} + x^{33} + x^{34} - x^{35} + x^{36} - x^{37} - x^{38} + x^{39} + x^{40} - x^{41} - x^{42} + x^{43} - x^{44} \text{ etc.}$$

ubi notandum est, quamlibet potestatem exponentis imparis x^{2n+1} contrarium habere signum ei, quod habet potestas x^{2n}, hujusque signum perpetuo convenire cum signo potestatis x^n; unde cujusvis potestatis signum facile assignabitur. Uti si quaeratur signum potestatis hujus x^{1745}, erit respectu ad sola signa habito:

$$x^{1745} = -x^{1744} = -x^{872} = -x^{436} = -x^{218} = -x^{109} = +x^{108} = +x^{54} = +x^{27} = -x^{26} = -x^{13}$$
$$= +x^{12} = +x^6 = +x^3 = -x^2 = -x^1$$

signum ergo potestatis x^{1745} contrarium est signo potestatis x^1, quod cum sit $-$, erit id $+$.

Tabula indicans, quot variis modis quilibet numerus n ex numeris 1, 2, 3, 4,.....m per additionem produci possit, seu exhibens valores formulae $n^{(m)}$.

	Valores numeri n															
m.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	0 1	1 2	1 2	2 3	2 3	3 4	3 4	4 5	4 5	5 6	5 6	6 7	6 7	7 8	7 8
3	1	1	2	1 3	1 4	2 5	3 7	4 8	5 10	7 12	8 14	10 16	12 19	14 21	16 24	19 27
4	1	1	2	3	1 5	1 6	2 9	3 11	5 15	6 18	9 23	11 27	15 34	18 39	23 47	27 54
5	1	1	2	3	5	1 7	1 10	2 13	3 18	5 23	7 30	10 37	13 47	18 57	23 70	30 84
6	1	1	2	3	5	7	1 11	1 14	2 20	3 26	5 35	7 44	11 58	14 71	20 90	26 110
7	1	1	2	3	5	7	11	1 15	1 21	2 28	3 38	5 49	7 65	11 82	15 105	21 131
8	1	1	2	3	5	7	11	15	1 22	1 29	2 40	3 52	5 70	7 89	11 116	15 146
9	1	1	2	3	5	7	11	15	22	1 30	1 41	2 54	3 73	5 94	7 123	11 157
10	1	1	2	3	5	7	11	15	22	30	1 42	1 55	2 75	3 97	5 128	7 164
11	1	1	2	3	5	7	11	15	22	30	42	1 56	1 76	2 99	3 131	5 169
12	1	1	2	3	5	7	11	15	22	30	42	56	1 77	1 100	2 133	3 172
13	1	1	2	3	5	7	11	15	22	30	42	56	77	1 101	1 134	2 174
14	1	1	2	3	5	7	11	15	22	30	42	56	77	101	1 135	1 175
15	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	1 176
16	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
17	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
18	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
19	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
20	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176
∞	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176

m.	16	17	18	19	20	21	22	23	24	25	26
1	1	1	1	1	1	1	1	1	1	1	1
	8	8	9	9	10	10	11	11	12	12	13
2	9	9	10	10	11	11	12	12	13	13	14
	21	24	27	30	33	37	40	44	48	52	56
3	30	33	37	40	44	48	52	56	61	65	70
	34	39	47	54	64	72	84	94	108	120	136
4	64	72	84	94	108	120	136	150	169	185	206
	37	47	57	70	84	101	119	141	164	192	221
5	101	119	141	164	192	221	255	291	333	377	427
	35	44	58	71	90	110	136	163	199	235	282
6	136	163	199	235	282	331	391	454	532	612	709
	28	38	49	65	82	105	131	164	201	248	300
7	164	201	248	300	364	436	522	618	733	860	1009
	22	29	40	52	70	89	116	146	186	230	288
8	186	230	288	352	434	525	638	764	919	1090	1297
	15	22	30	41	54	73	94	123	157	201	252
9	201	252	318	393	488	598	732	887	1076	1291	1549
	11	15	22	30	42	55	75	97	128	164	212
10	212	267	340	423	530	653	807	984	1204	1455	1761
	7	11	15	22	30	42	56	76	99	131	169
11	219	278	355	445	560	695	863	1060	1303	1586	1930
	5	7	11	15	22	30	42	56	77	100	133
12	224	285	366	460	582	725	905	1116	1380	1686	2063
	3	5	7	11	15	22	30	42	56	77	101
13	227	290	373	471	597	747	935	1158	1436	1763	2164
	2	3	5	7	11	15	22	30	42	56	77
14	229	293	378	478	608	762	957	1188	1478	1819	2241
	1	2	3	5	7	11	15	22	30	42	56
15	230	295	381	483	615	773	972	1210	1508	1861	2297
	1	1	2	3	5	7	11	15	22	30	42
16	231	296	383	486	620	780	983	1225	1530	1891	2339
		1	1	2	3	5	7	11	15	22	30
17	231	297	384	488	623	785	990	1236	1545	1913	2369
			1	1	2	3	5	7	11	15	22
18	231	297	385	489	625	788	995	1243	1556	1928	2391
				1	1	2	3	5	7	11	15
19	231	297	385	490	626	790	998	1248	1563	1939	2406
					1	1	2	3	5	7	11
20	231	297	385	490	627	791	1000	1251	1568	1946	2417
						1	2	4	7	12	19
∞	231	297	385	490	627	792	1002	1255	1575	1958	2436

m.	27	28	29	30	31	32	33	34	35	36	37
1	1	1	1	1	1	1	1	1	1	1	1
2	13 14	14 15	14 15	15 16	15 16	16 17	16 17	17 18	17 18	18 19	18 19
3	61 75	65 80	70 85	75 91	80 96	85 102	91 108	96 114	102 120	108 127	114 133
4	150 225	169 249	185 270	206 297	225 321	249 351	270 378	297 411	321 441	351 478	378 511
5	255 480	291 540	333 603	377 674	427 748	480 831	540 918	603 1014	674 1115	748 1226	831 1342
6	331 811	391 931	454 1057	532 1206	612 1360	709 1540	811 1729	931 1945	1057 2172	1206 2432	1360 2702
7	364 1175	436 1367	522 1579	618 1824	733 2093	860 2400	1009 2738	1175 3120	1367 3539	1579 4011	1824 4526
8	352 1527	434 1801	525 2104	638 2462	764 2857	919 3319	1090 3828	1297 4417	1527 5066	1801 5812	2104 6630
9	318 1845	393 2194	488 2592	598 3060	732 3589	887 4206	1076 4904	1291 5708	1549 6615	1845 7657	2194 8824
10	267 2112	340 2534	423 3015	530 3590	653 4242	807 5013	984 5888	1204 6912	1455 8070	1761 9418	2112 10936
11	219 2331	278 2812	355 3370	445 4035	560 4802	695 5708	863 6751	1060 7972	1303 9373	1586 11004	1930 12866
12	172 2503	224 3036	285 3655	366 4401	460 5262	582 6290	725 7476	905 8877	1116 10489	1380 12384	1686 14552
13	134 2637	174 3210	227 3882	290 4691	373 5635	471 6761	597 8073	747 9624	935 11424	1158 13542	1436 15988
14	101 2738	135 3345	175 4057	229 4920	293 5928	378 7139	478 8551	608 10232	762 12186	957 14499	1188 17176
15	77 2815	101 3446	135 4192	176 5096	230 6158	295 7434	381 8932	483 10715	615 12801	773 15272	972 18148
16	56 2871	77 3523	101 4293	135 5231	176 6334	231 7665	296 9228	383 11098	486 13287	620 15892	780 18928
17	42 2913	56 3579	77 4370	101 5432	135 6469	176 7841	231 9459	297 11395	384 13671	488 16380	623 19551
18	30 2943	42 3621	56 4426	77 5409	101 6570	135 7976	176 9635	231 11626	297 13968	385 16765	489 20040
19	22 2965	30 3651	42 4468	56 5465	77 6647	101 8077	135 9770	176 11802	231 14199	297 17062	385 20425
20	15 2980	22 3673	30 4498	42 5507	56 6703	77 8154	101 9871	135 11937	176 14375	231 17293	297 20722
∞	30 3010	45 3718	67 4565	97 5604	139 6842	195 8349	272 10143	373 12310	508 14883	684 17977	915 21637

m.	38	39	40	41	42	43	44	45	46	47	48
1	1	1	1	1	1	1	1	1	1	1	1
2	19 20	19 20	20 21	20 21	21 22	21 22	22 23	22 23	23 24	23 24	24 25
3	120 140	127 147	133 154	140 161	147 169	154 176	161 184	169 192	176 200	184 208	192 217
4	411 551	441 588	478 632	511 672	551 720	588 764	632 816	672 864	720 920	764 972	816 1033
5	918 1469	1014 1602	1115 1747	1226 1898	1342 2062	1469 2233	1602 2418	1747 2611	1898 2818	2062 3034	2233 3266
6	1540 3009	1729 3331	1945 3692	2172 4070	2432 4494	2702 4935	3009 5427	3331 5942	3692 6510	4070 7104	4494 7760
7	2093 5102	2400 5731	2738 6430	3120 7190	3539 8033	4011 8946	4526 9953	5102 11044	5731 12241	6430 13534	7190 14950
8	2462 7564	2857 8588	3319 9749	3828 11018	4417 12450	5066 14012	5812 15765	6630 17674	7564 19805	8588 22122	9749 24699
9	2592 10156	3060 11648	3589 13338	4206 15224	4904 17354	5708 19720	6615 22380	7657 25331	8824 28629	10156 32278	11648 36347
10	2534 12690	3015 14663	3590 16928	4242 19466	5013 22367	5888 25608	6912 29292	8070 33401	9418 38047	10936 43214	12690 49037
11	2331 15021	2812 17475	3370 20298	4035 23501	4802 27169	5708 31316	6751 36043	7072 41373	9373 47420	11004 54218	12866 61903
12	2063 17084	2503 19978	3036 23334	3655 27156	4401 31570	5262 36578	6290 42333	7476 48849	8877 56297	10489 64707	12384 74287
13	1763 18847	2164 22142	2637 25971	3210 30366	3882 35452	4691 41269	5635 47968	6761 55610	8073 64370	9624 74331	11424 85711
14	1478 20325	1819 23961	2241 28212	2738 33104	3345 38797	4057 45326	4920 52888	5928 61538	7139 71509	8551 82882	10232 95943
15	1210 21535	1508 25469	1861 30073	2297 35401	2815 41612	3446 48772	4192 57080	5096 66634	6158 77667	7434 90316	8932 104875
16	983 22518	1225 26694	1530 31603	1891 37292	2339 43951	2871 51643	3523 60603	4293 70927	5231 82898	6334 96650	7665 112540
17	785 23303	990 27684	1236 32839	1545 38837	1913 45864	2369 54012	2913 63516	3579 74506	4370 87268	5332 101982	6469 119009
18	625 23928	788 28472	995 33834	1243 40080	1556 47420	1928 55940	2391 65907	2943 77449	3621 90889	4426 106408	5409 124418
19	490 24418	626 29098	790 34624	998 41078	1248 48668	1563 57503	1939 67846	2406 79855	2965 93854	3651 110059	4468 128886
20	385 24803	490 29588	627 35251	791 41869	1000 49668	1251 58754	1568 69414	1946 81801	2417 96271	2980 113039	3673 132559
∞	1212 26015	1597 31185	2087 37338	2714 44583	3506 53174	4507 63261	5761 75175	7333 89134	9287 105558	11715 124754	14714 147273

m.	49	50	51	52	53	54	55	56	57	58	59
1	1	1	1	1	1	1	1	1	1	1	1
2	24 25	25 26	25 26	26 27	26 27	27 28	27 28	28 29	28 29	29 30	29 30
3	200 225	208 234	217 243	225 252	234 261	243 271	252 280	261 290	271 300	280 310	290 320
4	864 1089	920 1154	972 1215	1033 1285	1089 1350	1154 1425	1215 1495	1285 1575	1350 1650	1425 1735	1495 1815
5	2418 3507	2611 3765	2818 4033	3034 4319	3266 4616	3507 4932	3765 5260	4033 5608	4319 5969	4616 6351	4932 6747
6	4935 8442	5427 9192	5942 9975	6510 10829	7104 11720	7760 12692	8442 13702	9192 14800	9975 15944	10829 17180	11720 18467
7	8033 16475	8946 18138	9953 19928	11044 21873	12241 23961	13534 26226	14950 28652	16475 31275	18138 34082	19928 37108	21873 40340
8	11018 27493	12450 30588	14012 33940	15765 37638	17674 41635	19805 46031	22122 50774	24699 55974	27493 61575	30588 67696	33940 74280
9	13338 40831	15224 45812	17354 51294	19720 57358	22380 64015	25331 71362	28629 79403	32278 88252	36347 97922	40831 108527	45812 120092
10	14663 55494	16928 62740	19466 70760	22367 79725	25608 89623	29292 100654	33401 112804	38047 126299	43214 141136	49037 157564	55494 175586
11	15021 70515	17475 80215	20298 91058	23501 103226	27169 116792	31316 131970	36043 148847	41373 167672	47420 188556	54218 211782	61903 237489
12	14552 85067	17084 97299	19978 111036	23334 126560	27156 143948	31570 163540	36578 185425	42333 210005	48849 237405	56297 268079	64707 302196
13	13542 98609	15988 113287	18847 129883	22142 148702	25971 169919	30366 193906	35452 220877	41269 251274	47968 285373	55610 323689	64370 366566
14	12186 110795	14499 127786	17176 147059	20325 169027	23961 193880	28212 222118	33104 253981	38797 290071	45326 330699	52888 376577	61538 428104
15	10715 121510	12801 140587	15272 162331	18148 187175	21535 215415	25469 247587	30073 284054	35401 325472	41612 372311	48772 425349	57080 485184
16	9228 130738	11098 151685	13287 175618	15892 203067	18928 234343	22518 270105	26694 310748	31603 357075	37292 409603	43951 469300	51643 536827
17	7841 138579	9459 161144	11395 187013	13671 216738	16380 250723	19551 289656	23303 334051	27684 384759	32839 442442	38837 508137	45864 582691
18	6570 145149	7976 169120	9635 196648	11626 228364	13968 264691	16765 306421	20040 354091	23928 408687	28472 470914	33834 541971	40080 622771
19	5465 150614	6647 175767	8077 204725	9770 238134	11802 276493	14199 320620	17062 371153	20425 429112	24418 495332	29098 571069	34624 657395
20	4498 155112	5507 181274	6703 211428	8154 246288	9871 286364	11937 332557	14375 385528	17293 446405	20722 516054	24803 595872	29588 686983
∞	18413 173525	22952 204226	28515 239943	35301 281589	43567 329931	53598 386155	63748 451276	80418 526823	98100 614134	119348 715229	144837 831820

X.

De numeris amicabilibus.

(Opuscula varii argum. II. 1750. p. 23.)

§ 1. Bini numeri vocantur amicabiles, si ita sint comparati, ut summa partium aliquotarum unius aequalis sit alteri numero, et vicissim, summa partium aliquotarum alterius priori numero aequetur. Sic isti numeri 220 et 284 sunt amicabiles; prioris enim 220 partes aliquotae junctim sumtae: $1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110$ faciunt 284; et hujus numeri 284 partes aliquotae: $1 + 2 + 4 + 71 + 142$ producunt priorem numerum 220.

§ 2. **Scholion.** Stifelius, qui primus hujusmodi numerorum mentionem fecit, casu hos duos numeros 220 et 284 contemplatus ad hanc speculationem deductus videtur; analysin enim ineptam existimat, cujus ope plura istiusmodi numerorum paria inveniantur. Cartesius vero analysin ad hoc negotium accommodare est conatus, regulamque tradidit, qua tria talium numerorum paria elicuit, neque praeterea Schotenius, qui multum in hac investigatione desudasse videtur, plura eruere valuit. Post haec tempora nemo fere geometrarum ad hanc quaestionem magis evolvendam operam impendisse reperitur. Cum autem nullum sit dubium quin analysis quoque ex hac parte incrementa non contemnenda sit consecutura, si methodus aperiatur, qua multo plura hujusmodi numerorum paria investigare liceat, haud abs re fore arbitror, si methodos quasdam huc spectantes, in quas forte incidi, communicavero. In hunc finem autem sequentia praemittere necesse est.

§ 3. **Hypothesis.** Si n denotet numerum quemcunque integrum positivum, cujusmodi numeri hic semper sunt intelligendi, omnium ejus divisorum summam hoc signo $\int n$ indicabo, ita ut character $\int$ numero cuipiam praefixus summam omnium ejusdem numeri divisorum denotet: sic erit $\int 6 = 1 + 2 + 3 + 6 = 12$.

§ 4. **Coroll. 1.** Quoniam inter divisores cujusvis numeri hic ipse numerus refertur, partes aliquotae autem censentur divisores ipso numero excepto, manifestum est summam partium aliquotarum numeri n exprimi per $\int n - n$.

§ 5. **Coroll. 2.** Quoniam numerus primus nullos alios divisores admittit praeter unitatem et se ipsum, si n sit numerus primus erit $\int n = 1 + n$. Cum autem casu $n = 1$ sit $\int 1 = 1$, patet unitatem non recte numeris primis annumerari.

§. 6. **Lemma 1.** Si m et n fuerint numeri inter se primi, ut praeter unitatem nullum habeant divisorem communem, tum erit $\int mn = \int m . \int n$, seu summa divisorum producti mn aequalis est producto ex summis divisorum utriusque numeri m et n. Productum enim mn primo habet singulos divisores utriusque factoris m et n, tum vero insuper divisibile est per producta ex singulis divisoribus numeri m in singulos divisores numeri n. Hi vero omnes ipsius mn divisores junctim prodeunt si $\int m$ per $\int n$ multiplicetur.

§ 7. **Coroll. 1.** Si numerorum m et n uterque sit primus, ideoque $\int m = 1 + m$ et $\int n = 1 + n$, erit summa divisorum producti

$$\int mn = (1 + m)(1 + n) = 1 + m + n + mn.$$

Si praeterea p sit numerus primus diversus ab m et n, erit

$$\int mnp = \int mn . \int p = \int m . \int n . \int p = (1 + m)(1 + n)(1 + p).$$

Hincque summa divisorum cujusque numeri, qui est productum ex quotcunque numeris primis diversis, facile assignabitur.

§ 8. **Coroll. 2.** Si m, n et p non quidem sint numeri primi, sed tamen ejusmodi, ut praeter unitatem nullum habeant divisorem communem, tum mn et p erunt numeri inter se primi, ac propterea $\int mnp = \int mn . \int p$. Cum autem sit $\int mn = \int m . \int n$, erit $\int mnp = \int m . \int n . \int p$.

§ 9. **Scholion.** Nisi factores m, n, p sunt numeri inter se primi, summa divisorum producti, prout per lemma indicatur, non est justa. Cum enim secundum lemma singuli divisores factorum m, n, p inter divisores producti mnp referantur, si haberent divisorem communem, is inter divisores producti bis numeraretur; at dum quaestio de summa divisorum cujuspiam numeri instituitur, nullum divisorem bis numerare oportet. Hinc si m et n sint numeri primi, ac $m = n$, non erit

$$\int nn = \int n . \int n = (1 + n)^2 = 1 + 2n + nn,$$

sed habebitur $\int nn = 1 + n + nn$, neque divisorem n bis poni convenit. Cum igitur per hoc lemma summa divisorum cujusque numeri, qui est productum ex quotcunque numeris primis diversis, recte assignetur, residuum est, ut pro factoribus aequalibus regula tradatur, cujus ope summa divisorum producti definiri queat.

§ 10. **Lemma 2.** Si n sit numerus primus, erit

$$\int n^2 = 1 + n + n^2, \quad \int n^3 = 1 + n + n^2 + n^3, \quad \int n^4 = 1 + n + n^2 + n^3 + n^4,$$

et generatim erit

$$\int n^k = 1 + n + n^2 + \ldots + n^k = \frac{n^{k+1} - 1}{n - 1}.$$

§ 11. **Coroll. 1.** Cum sit $\int n = 1 + n$, erit $\int n^2 = \int n + n^2$, vel etiam $\int n^2 = 1 + n \int n$. Simili modo erit $\int n^3 = \int n^2 + n^3$, vel etiam $\int n^3 = 1 + n \int n^2$; porroque $\int n^4 = \int n^3 + n^4$ seu $\int n^4 = 1 + n \int n^3$ et ita porro. Sicque ex cognita summa divisorum cujusque potestatis n^k facile summa divisorum potestatis sequentis n^{k+1} assignatur, cum sit $\int n^{k+1} = \int n^k + n^{k+1}$ seu $\int n^{k+1} = 1 + n \int n^k$.

§ 12. **Coroll. 2.** Quo summae divisorum facilius per factores exprimi queant, notandum est esse

$$\int n^3 = (1 + n)(1 + n^2) = (1 + n^2) \int n$$
$$\int n^5 = (1 + n^2 + n^4) \int n$$
$$\int n^7 = (1 + n^2 + n^4 + n^6) \int n = (1 + n^4)(1 + n^2) \int n.$$

Sicque summae divisorum potestatum imparium semper per factores exhiberi possunt: at potestatum parium summae divisorum quandoque erunt numeri primi.

§ 13. **Coroll. 3.** Hinc igitur facile tabula condi poterit, qua non solum numerorum primorum, sed etiam potestatum ipsorum summae divisorum exhibeantur. Cujusmodi tabulam hic adjicere visum est, in qua omnium numerorum primorum millenario non majorum, eorumque potestatum ad tertiam usque et altiores pro minoribus numeris summae divisorum per factores expressae traduntur.

Num.	Summa divisorum.	Num.	Summa divisorum.	Num.	Summa divisorum.
2	3.	3	2^2.	11	2^2. 3.
2^2	7.	3^2	13.	11^2	7. 19.
2^3	3. 5.	3^3	2^3. 5.	11^3	2^3. 3. 61.
2^4	31.	3^4	11^2.	11^4	5. 3221.
2^5	3^2. 7.	3^5	2^2. 7. 13.	11^5	2^2. 3^2. 7. 19. 37.
2^6	127.	3^6	1093.	11^6	43. 45319.
2^7	3. 5. 17.	3^7	2^4. 5. 41.	11^7	2^4. 3. 61. 7321.
2^8	7. 73.	3^8	13. 757.	11^8	7. 19. 1772893.
2^9	3. 11. 31.	3^9	2^2. 11^2. 61.	11^9	2^2. 3. 5. 3221. 13421.
2^{10}	23. 89.	3^{10}	23. 3851.	13	2. 7.
2^{11}	3^2. 5. 7. 13.	3^{11}	2^3. 5. 7. 13. 73.	13^2	3. 61.
2^{12}	8191.	3^{12}	797161.	13^3	2^2. 5. 7. 17.
2^{13}	3. 43. 127.	3^{13}	2^2. 547. 1093.	13^4	30941.
2^{14}	7. 31. 151.	3^{14}	11^2. 13. 4561.	13^5	2. 3. 7. 61. 157.
2^{15}	3. 5. 17. 257.	3^{15}	2^5. 5. 17. 41. 193.	13^6	5229043.
2^{16}	131071.			13^7	2^3. 5. 7. 17. 14281.
2^{17}	3^3. 7. 19. 73.	5	2. 3.	17	2. 3^2.
2^{18}	524287.	5^2	31.	17^2	307.
2^{19}	3. 5^2. 11. 31. 41.	5^3	2^2. 3. 13.	17^3	2^2. 3^2. 5. 29.
2^{20}	7^2. 127. 337.	5^4	11. 71.	17^4	88741.
2^{21}	3. 23. 89. 683.	5^5	2. 3^2. 7. 31.	17^5	2. 3^3. 7. 13. 307.
2^{22}	47. 178481.	5^6	19531.	19	2^2. 5.
2^{23}	3^2. 5. 7. 13. 17. 241.	5^7	2^3. 3. 13. 313.	19^2	3. 127.
2^{24}	31. 601. 1801.	5^8	19. 31. 829.	19^3	2^3. 5. 181.
2^{25}	3. 2731. 8191.	5^9	2. 3. 11. 71. 521.	19^4	151. 911.
2^{26}	7. 73. 262657.			19^5	2^2. 3. 5. 7^3. 127.
2^{27}	3. 5. 29. 43. 113. 127.	7	2^3.	23	2^3. 3.
2^{28}	233. 1103. 2089.	7^2	3. 19.	23^2	7. 79.
2^{29}	3^2. 7. 11. 31. 151. 331.	7^3	2^4. 5^2.	23^3	2^4. 3. 5. 53.
2^{30}	2147483647.	7^4	2801.	23^4	292561.
2^{31}	3. 5. 17. 257. 65537.	7^5	2^3. 3. 19. 43.		
2^{32}	7. 23. 89. 599479.	7^6	29. 4733.		
2^{33}	3. 43691. 131071.	7^7	2^5. 5^2. 1201.		
2^{34}	31. 71. 127. 122921.	7^8	3^2. 19. 37. 1063.	29	2. 3. 5.
2^{35}	3^3. 5. 7. 13. 19. 37. 73. 109.	7^9	2^3. 11. 191. 2801.	29^2	13. 67.
2^{36}	223. 616318177.	7^{10}	329554457.	29^3	2^2. 3. 5. 421.

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
31	2^5.	83	$2^2. 3. 7$.	139	$2^2. 5. 7$.
31^2	3. 331.	83^2	19. 367.	139^2	3. 13. 499.
31^3	$2^6. 13. 37$.	83^3	$2^3. 3. 5. 7. 13. 53$.	139^3	$2^3. 5. 7. 9661$.
37	2. 19.	89	$2. 3^2. 5$.	149	$2. 3. 5^2$.
37^2	3. 7. 67.	89^2	8011.	149^2	7. 31. 103.
37^3	$2^2. 5. 2603$.	89^3	$2^2. 3^2. 5. 17. 233$.	149^3	$2^2. 3. 5^2. 11. 101$.
41	2. 3. 7.	97	$2. 7^2$.	151	$2^3. 19$.
41^2	1723.	97^2	3. 3169.	151^2	3. 7. 1093.
41^3	$2^2. 3. 7. 29$.	97^3	$2^2. 5. 7^2. 941$.	151^3	$2^4. 13. 19. 877$.
43	$2^2. 11$.	101	2. 3. 17.	157	2. 79.
43^2	3. 631.	101^2	10303.	157^2	3. 8269.
43^3	$2^3. 5^2. 11. 37$.	101^3	$2^2. 3. 17. 5101$.	157^3	$2^2. 5^2. 17. 29. 79$.
47	$2^4. 3$.	103	$2^3. 13$.	163	$2^2. 41$.
47^2	37. 61.	103^2	3. 3571.	163^2	3. 7. 19. 67.
47^3	$2^5. 3. 5. 13. 17$.	103^3	$2^4. 5. 13. 1061$.	163^3	$2^3. 5. 41. 2657$.
53	$2. 3^3$.	107	$2^2. 3^3$.	167	$2^3. 3. 7$.
53^2	7. 409.	107^2	7. 13. 127.	167^2	28057.
53^3	$2^2. 3^3. 5. 281$.	107^3	$2^3. 3^3. 5^2. 229$.	167^3	$2^4. 3. 5. 7. 2789$.
59	$2^2. 3. 5$.	109	2. 5. 11.	173	2. 3. 29.
59^2	3541.	109^2	3. 7. 571.	173^2	67. 449.
59^3	$2^3. 3. 5. 1741$.	109^3	$2^2. 5. 11. 13. 457$.	173^3	$2^2. 3. 5. 29. 41. 73$.
61	2. 31.	113	2. 3. 19.	179	$2^2. 3^2. 5$.
61^2	3. 13. 97.	113^2	13. 991.	179^2	7. 4603.
61^3	$2^2. 31. 1861$.	113^3	$2^2. 3. 5. 19. 1277$.	179^3	$2^3. 3^2. 5. 37. 433$.
67	$2^2. 17$.	127	2^7.	181	2. 7. 13.
67^2	$3. 7^2. 31$.	127^2	3. 5419.	181^2	3. 79. 139.
67^3	$2^3. 5. 17. 449$.	127^3	$2^8. 5. 1613$.	181^3	$2^2. 7. 13. 16381$.
71	$2^3. 3^2$.	131	$2^2. 3. 11$.	191	$2^6. 3$.
71^2	5113.	131^2	17293.	191^2	$7. 13^2. 31$.
71^3	$2^4. 3^2. 2521$.	131^3	$2^3. 3. 11. 8581$.	191^3	$2^7. 3. 17. 29. 37$.
73	2. 37.	137	2. 3. 23.	193	2. 97.
73^2	3. 1801.	137^2	7. 37. 73.	193^2	3. 7. 1783.
73^3	$2^2. 5. 13. 37. 41$.	137^3	$2^2. 3. 5. 23. 1877$.	193^3	$2^2. 5^3. 97. 149$.

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
197	$2.3^2.11.$	263	$2^3.3.11.$	331	$2^2.83.$
197^2	19. 2053.	263^2	$7^2.13.109.$	331^2	3. 7. 5233.
197^3	$2^2.3^2.5.11.3881.$	263^3	$2^4.3.5.11.6917.$	331^3	$2^3.29.83.1889.$
199	$2^3.5^2.$	269	$2.3^3.5.$	337	$2.13^2.$
199^2	3. 13267.	269^2	13. 37. 151.	337^2	3. 43. 883.
199^3	$2^4.5^2.19801.$	269^3	$2^2.3^3.5.97.373.$	337^3	$2^2.5.13^2.41.277.$
211	$2^2.53.$	271	$2^4.17.$	347	$2^2.3.29.$
211^2	3. 13. 31. 37.	271^2	3. 24571.	347^2	7. 13. 1327.
211^3	$2^3.53.113.197.$	271^3	$2^5.17.36721.$	347^3	$2^3.3.5.29.12041.$
223	$2^5.7.$	277	2. 139.	349	$2.5^2.7.$
223^2	3. 16651.	277^2	3. 7. 19. 193.	349^2	3. 19. 2143.
223^3	$2^6.5.7.4973.$	277^3	$2^2.5.139.7673.$	349^3	$2^2.5^2.7.60901.$
227	$2^2.3.19.$	281	2. 3. 47.	353	2. 3. 59.
227^2	73. 709.	281^2	109. 727.	353^2	19. 6577.
227^3	$2^3.3.5.19.5153.$	281^3	$2^2.3.13.47.3037.$	353^3	$2^2.3.5.17.59.733.$
229	2. 5. 23.	283	$2^2.71.$	359	$2^3.3^2.5.$
229^2	3. 97. 181.	283^2	3. 73. 367.	359^2	7. 37. 499.
229^3	$2^2.5.13.23.2017.$	283^3	$2^3.5.71.8009.$	359^3	$2^4.3^2.5.13.4957.$
233	$2.3^2.13.$	293	$2.3.7^2.$	367	$2^4.23.$
233^2	7. 7789.	293^2	86143.	367^2	3. 13. 3463.
233^3	$2^2.3^2.5.13.61.89.$	293^3	$2^2.3.5^2.7^2.17.101.$	367^3	$2^5.5.23.13469.$
239	$2^4.3.5.$	307	$2^2.7.11.$	373	2. 11. 17.
239^2	19. 3019.	307^2	3. 43. 733.	373^2	$3.7^2.13.73.$
239^3	$2^5.3.5.13^4.$	307^3	$2^3.5^3.7.11.13.29.$	373^3	$2^2.5.11.17.13913.$
241	$2.11^2.$	311	$2^3.3.13.$	379	$2^2.5.19.$
241^2	3. 19441.	311^2	19. 5107.	379^2	3. 61. 787.
241^3	$2^2.11^2\ 113.257.$	311^3	$2^4.3.13.137.353.$	379^3	$2^3.5.19.71821.$
251	$2^2.3^2.7.$	313	2. 157.	383	$2^7.3.$
251^2	43. 1471.	313^2	$3.181^2.$	383^2	147073.
251^3	$2^3.3^2.7.17^2.109.$	313^3	$2^2.5.97.101.157.$	383^3	$2^8.3.5.14669.$
257	2. 3. 43.	317	2. 3. 53.	389	2. 3. 5. 13.
257^2	61. 1087.	317^2	7. 14401.	389^2	7. 21673.
257^3	$2^2.3.5^2.43.1321.$	317^3	$2^2.3.5.13.53.773.$	389^3	$2^2.3.5.13.29.2609.$

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
397	2. 199.	461	2. 3. 7. 11.	541	2. 271.
397^2	3. 31. 1699.	461^2	373. 571.	541^2	3. 7. 13963.
397^3	2^2. 5. 199. 15761.	461^3	2^2. 3. 7. 11106261.	541^3	2^2. 13. 271. 11257.
401	2. 3. 67.	463	2^4. 29.	547	2^2. 137.
401^2	7. 23029.	463^2	3. 19. 3769.	547^2	3. 163. 613.
401^3	2^2. 3. 37. 41. 53. 67.	463^3	2^5. 5. 13. 17. 29. 97.	547^3	2^3. 5. 137. 29921.
409	2. 5. 41.	467	2^2. 3^2. 13.	557	2. 3^2. 31.
409^2	3. 55897.	467^2	19. 11503.	557^2	7^2. 6343.
409^3	2^2. 5. 41. 83641.	467^3	2^3. 3^2. 5. 13. 113. 193.	557^3	2^2. 3^2. 5^3. 17. 31. 73.
419	2^2. 3. 5. 7.	479	2^5. 3. 5.	563	2^2. 3. 47.
419^2	13. 13537.	479^2	43. 5347.	563^2	31. 10243.
419^3	2^3. 3. 5. 7. 41. 2141.	479^3	2^6. 3. 5. 89. 1289.	563^3	2^3. 3. 5. 29. 47. 1093.
421	2. 211.	487	2^3. 61.	569	2. 3. 5. 19.
421^2	3. 59221.	487^2	3. 7. 11317.	569^2	7^2. 6619.
421^3	2^2. 13. 17. 211. 401.	487^3	2^4. 5. 37. 61. 641.	569^3	2^2 3. 5. 19. 161881.
431	2^4. 3^3.	491	2^2. 3. 41.	571	2^2. 11. 13.
431^2	7. 67. 397.	491^2	37. 6529.	571^2	3. 7. 103. 151.
431^3	2^5. 3^3. 293. 317.	491^3	2^3. 3. 41. 149. 809.	571^3	2^3. 11. 13. 163041.
433	2. 7. 31.	499	2^2. 5^3.	577	2. 17^2.
433^2	3. 37. 1693.	499^2	3. 7. 109^2.	577^2	3. 19. 5851.
433^3	2^2. 5. 7. 31. 18749.	499^3	2^3. 5^3. 13. 61. 157.	577^3	2^2. 5. 13^2. 17^2. 197.
439	2^3. 5. 11.	503	2^3. 3^2. 7.	587	2^2. 3. 7^2.
439^2	3. 31^2. 67.	503^2	13. 19501.	587^2	547. 631.
439^3	2^4. 5. 11. 173. 557.	503^3	2^4. 3^2. 5. 7. 25301.	587^3	2^3. 3. 5. 7^2. 34457.
443	2^2. 3. 37.	509	2. 3. 5. 17.	593	2. 3^3. 11.
443^2	7. 28099.	509^2	43. 6037.	593^2	163. 2161.
443^3	2^3. 3. 5^4. 37. 157.	509^3	2^2. 3. 5. 17. 281. 461.	593^3	2^2. 3^3. 5^2. 11. 13. 541.
449	2. 3^2. 5^2.	521	2. 3^2. 29.	599	2^3. 3. 5^2.
449^2	97. 2083.	521^2	31^2. 283.	599^2	7. 51343.
449^3	2^2. 3^2. 5^2. 100801.	521^3	2^2. 3^2. 29. 135721.	599^3	2^4. 3. 5^2. 17. 61. 173.
457	2. 229.	523	2^2. 131.	601	2. 7. 43.
457^2	3. 7. 9967.	523^2	3. 13. 7027.	601^2	3. 13. 9277.
457^3	2^2. 5^2. 229. 4177.	523^3	2^3. 5. 7. 131. 1609.	601^3	2^2. 7. 43. 313. 577.

Num.	Summa divisorum.	Num.	Summa divisorum.	Num.	Summa divisorum.
607	$2^5 . 19.$	673	$2 . 337.$	751	$2^4 . 47.$
607^2	$3 . 13 . 9463.$	673^2	$3 . 151201.$	751^2	$3 . 7 . 26893.$
607^3	$2^6 . 5^2 . 19 . 7369.$	673^3	$2^2 . 5 . 337 . 45293.$	751^3	$2^5 . 47 . 282001.$
613	$2 . 307.$	677	$2 . 3 . 113.$	757	$2 . 379.$
613^2	$3 . 125461.$	677^2	$459007.$	757^2	$3 . 13 . 14713.$
613^3	$2^2 . 5 . 53 . 307 . 709.$	677^3	$2^2 . 3 . 5 . 113 . 45833.$	757^3	$2^2 . 5^2 . 73 . 157 . 379.$
617	$2 . 3 . 103.$	683	$2^2 . 3^2 . 19.$	761	$2 . 3 . 127.$
617^2	$97 . 3931.$	683^2	$7 . 66739.$	761^2	$579883.$
617^3	$2^2 . 3 . 5 . 103 . 38069.$	683^2	$2^3 . 3^2 . 5 . 19 . 46649.$	761^3	$2^2 . 3 . 17 . 127 . 17033.$
619	$2^2 . 5 . 31.$	691	$2^2 . 173.$	769	$2 . 5 . 7 . 11.$
619^2	$3 . 19 . 6733.$	691^2	$3 . 19 . 8389.$	769^2	$3 . 31 . 6367.$
619^3	$2^3 . 5 . 13 . 31 . 14737.$	691^3	$2^3 . 173 . 193 . 1237.$	769^3	$2^2 . 5 . 7 . 11 . 71 . 17393.$
631	$2^3 . 79.$	701	$2 . 3^3 . 13.$	773	$2 . 3^2 . 43.$
631^2	$3 . 307 . 433.$	701^2	$492103.$	773^2	$598303.$
631^3	$2^4 . 79 . 199081.$	701^3	$2^2 . 3^3 . 13 . 17 . 97 . 149.$	773^3	$2^2 . 3^2 . 5 . 43 . 59753.$
641	$2 . 3 . 107.$	709	$2 . 5 . 71.$	787	$2^2 . 197.$
641^2	$7 . 58789.$	709^2	$3 . 7 . 23971.$	787^2	$3 . 37^2 . 151.$
641^3	$2^2 . 3 . 107 . 205441.$	709^3	$2^2 . 5 . 37 . 71 . 6793.$	787^3	$2^3 . 5 . 197 . 241 . 257.$
643	$2^2 . 7 . 23.$	719	$2^4 . 3^2 . 5.$	797	$2 . 3 . 7 . 19.$
643^2	$3 . 97 . 1423.$	719^2	$487 . 1063.$	797^2	$157 . 4051.$
643^3	$2^3 . 5^2 . 7 . 23 . 8269.$	719^3	$2^5 . 3^2 . 5 . 53 . 4877.$	797^3	$2^2 . 3 . 5 . 7 . 19 . 63521.$
647	$2^3 . 3^4.$	727	$2^3 . 7 . 13.$	809	$2 . 3^4 . 5.$
647^2	$211 . 1987.$	727^2	$3 . 176419.$	809^2	$7 . 13 . 19 . 379.$
647^3	$2^4 . 3^4 . 5 . 41 . 1021.$	727^3	$2^4 . 5 . 7 . 13 . 17 . 3109.$	809^3	$2^2 . 3^4 . 5 . 229 . 1429.$
653	$2 . 3 . 109.$	733	$2 . 367.$	811	$2 . 7 . 29.$
653^2	$7 . 13^2 . 19^2.$	733^2	$3 . 19 . 9439.$	811^2	$3 . 31 . 73 . 97.$
653^3	$2^2 . 3 . 5 . 109 . 42641.$	733^3	$2^2 . 5 . 13 . 367 . 4133.$	811^3	$2^3 . 7 . 13 . 29 . 41 . 617.$
659	$2^2 . 3 . 5 . 11.$	739	$2^2 . 5 . 37.$	821	$2 . 3 . 137.$
659^2	$13 . 33457.$	739^2	$3 . 7 . 26041.$	821^2	$7 . 229 . 421.$
659^3	$2^3 . 3 . 5 . 11 . 17 . 53 . 241.$	739^3	$2^3 . 5 . 37 . 273061.$	821^3	$2^2 . 3 . 137 . 337021.$
661	$2 . 331.$	743	$2^3 . 3 . 31.$	823	$2^3 . 103.$
661^2	$3 . 145861.$	743^2	$552793.$	823^2	$3 . 7 . 43 . 751.$
661^3	$2^2 . 331 . 218461.$	743^3	$2^4 . 3 . 5^2 . 31 . 61 . 181.$	823^3	$2^4 . 5 . 103 . 67733.$

Num.	Summa divisorum	Num.	Summa divisorum	Num.	Summa divisorum
827	$2^2. 3^2. 23.$	883	$2^2. 13. 17.$	953	$2. 3^2. 53.$
827^2	684757.	883^2	3. 260191.	953^2	181. 5023.
827^3	$2^3. 3^2. 5. 13. 23. 5261.$	883^3	$2^3. 5. 13. 17. 77969.$	953^3	$2^2. 3^2. 5. 53. 90821.$
829	2. 5. 83.	887	$2^3. 3. 37.$	967	$2^3. 11^2.$
829^2	3. 211. 1087.	887^2	13. 60589.	967^2	3. 67. 4657.
829^3	$2^2. 5. 17^2. 29. 41. 83.$	887^3	$2^4. 3. 5. 29. 37. 2713.$	967^3	$2^4. 5. 11^2. 13. 7193.$
839	$2^3. 3. 5. 7.$	907	$2^2. 227.$	971	$2^2. 3^5.$
839^2	704761.	907^2	3. 7. 39217.	971^2	13. 79. 919.
839^3	$2^4. 3. 5. 7. 109. 3229.$	907^3	$2^3. 5^2. 227. 16453.$	971^3	$2^3. 3^5. 197. 2393.$
853	2. 7. 61.	911	$2^4. 3. 19.$	977	2. 3. 163.
853^2	3. 43. 5647.	911^2	830833.	977^2	7. 136501.
853^3	$2^2. 5. 7. 13. 29. 61. 193.$	911^3	$2^5. 3. 19. 29. 41. 349.$	977^3	$2^2. 3. 5. 53. 163. 1801.$
857	2. 3. 11. 13.	919	$2^3. 5. 23.$	983	$2^3. 3. 41.$
857^2	735307.	919^2	3. 7. 13. 19. 163.	983^2	103. 9391.
857^3	$2^2. 3. 5^2. 11. 13. 37. 397.$	919^3	$2^4. 5. 23. 37. 101. 113.$	983^3	$2^4. 3. 5. 13. 41. 7433.$
859	$2^2. 5. 43.$	929	2. 3. 5. 31.	991	$2^5. 31.$
859^2	3. 246247.	919^2	157. 5503.	991^2	$3. 7. 13^2. 277.$
859^3	$2^3. 5. 43. 137. 2693.$	919^3	$2^2. 3. 5. 31. 431521.$	991^3	$2^6. 31. 491041.$
863	$2^5. 3^3.$	937	2. 7. 67.	997	2. 499.
863^2	$7^2. 15217.$	937^2	3. 292969.	997^2	3. 13. 31. 823.
863^3	$2^6. 3^3. 5. 13. 17. 337.$	937^3	$2^2. 5. 7. 67. 87797.$	997^3	$2^2. 5. 499. 99401.$
877	2. 439.	941	2. 3. 157.		
877^2	3. 7. 37. 991.	941^2	811. 1093.		
877^3	$2^2. 5. 439. 76913.$	941^3	$2^2. 3. 13. 157. 34057.$		
881	$2. 3^2. 7^2.$	947	$2^2. 3. 79.$		
881^2	19. 40897.	947^2	7. 277. 463.		
881^3	$2^2. 3^2. 7^2. 388081.$	947^3	$2^3. 3. 5. 79. 89681.$		

§ 14. **Scholion.** Usus hujus tabulae est amplissimus in quaestionibus circa divisores et partes aliquotas versantibus resolvendis. Ejus enim ope cujusque numeri propositi summa divisorum facili negotio inveniri potest, qua reperta, si inde ipse numerus propositus auferatur, remanebit ejus summa partium aliquotarum. Ex quo statim constat, hujus tabulae subsidio numeros amicabiles, quos sum traditurus, facile explorari posse, utrum sint justi nec ne? Quemadmodum autem ope hujus tabulae cujusvis numeri summa divisorum cognosci possit, in sequenti lemmate explicabo.

§ 15. **Lemma 3.** Proposito quocunque numero, ejus summa divisorum sequenti modo colligitur.

Cum omnis numerus sit vel primus, vel productum ex primis, resolvatur numerus propositus in suos factores primos, et qui inter se fuerint aequales, conjunctim exprimantur. Hoc modo numerus propositus semper ad hujusmodi formam redigetur $m^\alpha . n^\beta . p^\gamma . q^\delta$. etc. existentibus m, n, p, q etc. numeris primis. Posito ergo numero proposito $= N$, cum sit $N = m^\alpha . n^\beta . p^\gamma . q^\delta$. etc. et factores m^α, n^β, p^γ, q^δ, etc. inter se primi, erit $\int N = \int m^\alpha . \int n^\beta . \int p^\gamma . \int q^\delta$. etc., et valores $\int m^\alpha$, $\int n^\beta$, $\int p^\gamma$, $\int q^\delta$, etc. ex tabula adjuncta patebunt.

Exempl. 1. Sit numerus propositus $N = 360$.

Resoluto hoc numero in suos factores primos erit $N = 2^3 . 3^2 . 5$, ideoque

$$\int 360 = \int 2^3 . \int 3^2 . \int 5 = 3.5.13.2.3, \text{ ob } \int 2^3 = 3.5, \int 3^2 = 13, \int 5 = 2.3.$$

Unde his factoribus ordinatis fiet $\int 360 = 2.3^2.5.13 = 1170$.

Exempl. 2. Explorentur numeri 2620 et 2924 utrum sint amicabiles, nec ne?

Cum sit $2620 = 2^2.5.131$ et $2924 = 2^2.17.43$, examen ita instituetur

Numeri propositi	2620	2924
per factores expressi	$2^2.5.131$	$2^2.17.43$
summae divisorum.........	$7.6.132 = 5544$	$7.18.44 = 5544$
summae partium aliquotarum	2924	2620

Cum igitur summae partium aliquotarum sint numeri reciproce aequales, patet propositos numeros esse amicabiles.

§ 16. **Schollon.** His igitur praemissis, quae ad inventionem divisorum cujusque numeri pertinent, ipsum problema de investigatione numerorum amicabilium aggrediar, atque scrutabor, quemadmodum hujusmodi numeros ratione summae divisorum inter se comparatos esse oporteat, quo deinceps facilius eorum inventio per regulas post tradendas suscipi queat.

§ 17. **Problema generale.** Invenire numeros amicabiles, hoc est duos numeros hujus indolis, ut alter aequalis sit summae partium aliquotarum alterius.

Solutio. Sint m et n duo hujusmodi numeri amicabiles, et per hypothesin $\int m$ et $\int n$ summae divisorum eorumdem. Erit numeri m summa partium aliquotarum $= \int m - m$, et numeri n summa partium aliquotarum $= \int n - n$. Hinc ex natura numerorum amicabilium nascentur hae duae aequationes:

$$\int m - m = n \quad \text{et} \quad \int n - n = m, \quad \text{sive} \quad \int m = \int n = m + n.$$

Numeri ergo amicabiles m et n primo habere debent eandem summam divisorum, tum vero oportet, ut haec communis divisorum summa aequalis sit aggregato ipsorum numerorum $m + n$.

§ 18. **Coroll. 1.** Problema ergo huc reducitur, ut quaerantur duo ejusmodi numeri, qui habeant eandem divisorum summam, haecque aequalis sit aggregato ipsorum numerorum.

§ 19. **Coroll. 2.** Ipsa quidem problematis ratio exigit, ut bini numeri quaesiti sint inter se inaequales: sin autem desiderentur aequales, ut sit $m = n$, fiet $\int n = 2n$ et $\int n - n = n$: hujus scilicet numeri geminati n summa partium aliquotarum ipsi fiet aequalis, quae est proprietas numeri perfecti. Ergo quilibet numerus perfectus repetitus numeros exhibet amicabiles.

§ 20. **Coroll. 3.** Sin autem numeri amicabiles m et n, ut natura quaestionis postulat, sint inaequales, manifestum est, alterum esse redundantem, alterum deficientem; summa scilicet partium aliquotarum alterius ipso erit major, alterius vero ipso minor.

§ 21. **Scholion.** Ex hac quidem generali proprietate parum adjumenti consequimur ad numeros amicabiles inveniendos, eo quod ista analyseos species, cujus ope aequationem

$$\int m = \int n = m + n$$

evolvere liceat, etiam nunc penitus sit inculta. Ob quem defectum formulas magis particulares contemplari cogimur, ex quarum indole regulas speciales pro inventione numerorum amicabilium derivare liceat; quorsum etiam pertinet regula Cartesiana a Schotenio commemorata. Ac primo quidem, etiamsi non constet, utrum dentur numeri amicabiles inter se primi, nec ne? formulas generales ita restringam, ut numeri amicabiles factorem communem obtineant.

§ 22. **Problema particulare.** Invenire indolem numerorum amicabilium, qui communem habeant factorem.

Solutio. Sit a communis factor numerorum amicabilium, quorum alter ponatur $= am$, alter $= an$; sint vero tam m et a, quam n et a numeri inter se primi, ut utriusque divisorum summa per praecepta data reperiri queat. Cum igitur primo utriusque eadem esse debeat divisorum summa, fiet $\int a . \int m = \int a . \int n$, ideoque $\int m = \int n$. Deinde vero necesse est ut sit $\int a . \int m$ seu $\int a . \int n$ ipsorum numerorum aequalis aggregato $am + an$, unde habetur $\frac{a}{\int a} = \frac{\int m}{m+n} = \frac{\int n}{m+n}$. Positis ergo numeris amicabilibus am et an, primo esse oportet $\int m = \int n$, tum vero requiritur ut sit $a(m+n) = \int a . \int m$.

§ 23. **Coroll. 1.** Si ergo pro m et n ejusmodi numeri jam fuerint eruti, ut sit $\int m = \int n$, tum numerus a investigari debet, ut sit $\frac{a}{\int a} = \frac{\int m}{m+n}$, seu ex ratione, quam numerus ad summam divisorum suorum tenere debet, ipse numerus a erit investigandus.

§ 24. **Coroll. 2.** Si factor communis a fuerit datus, quaestio ad inventionem numerorum m et n reducitur, qui prouti vel primi, vel compositi ex duobus pluribusve primis assumuntur, quoniam tum divisorum summae actu exhiberi possunt, regulae speciales ad eos inveniendos tradi poterunt.

§ 25. **Coroll. 3.** Statim autem perspicitur utrumque numerum m et n primum esse non posse: quare casus simplicissimus exstat, si alter primus, alter vero productum ex duobus numeris primis assumatur. Tum uterque productum ex duobus, pluribusve numeris primis statui poterit, unde innumerae regulae speciales pro inveniendis numeris amicabilibus derivari poterunt.

§ 26. **Scholion.** Diversae ergo numerorum amicabilium formae, quae hinc nascuntur, sequenti modo repraesentari poterunt. Sit a utriusque communis factor, et p, q, r, s, etc. numeri primi, quorum nullus sit divisor communis factoris a, atque numerorum amicabilium formae erunt:

Forma prima $\begin{cases} apq \\ ar \end{cases}$ Forma secunda $\begin{cases} apq \\ ars \end{cases}$

Forma tertia $\begin{cases} apqr \\ as \end{cases}$ Forma quarta $\begin{cases} apqr \\ ast \end{cases}$

Forma quinta $\begin{cases} apqr \\ astu \end{cases}$ etc.

Quanquam numerus harum formarum in infinitum augeri potest, minime tamen hinc concludere licet, in his formis omnes numeros amicabiles contineri. Primum enim, dum hic litterae, p, q, r, s, t, etc. numeros primos diversos significant, non verisimile est, nullos dari numeros amicabiles, in quibus non occurrant potestates ejusdem numeri primi. Deinde pariter non constat, utrum non dentur numeri amicabiles, qui vel nullum habeant factorem communem a, vel in quibus factor hic non prorsus sit idem: veluti si darentur numeri amicabiles hujus formae $m^\alpha P$ et $m^\beta Q$, in quibus exponentes α et β essent diversi: quae forma propterea in superioribus non contineretur, etiamsi P et Q essent producta ex meris numeris primis inter se diversis. Ex his perspicitur quaestionem de numeris amicabilibus latissime patere, eamque ob hoc ipsum tam esse difficilem, ut solutio completa vix sit exspectanda. Solutionibus igitur particularibus equidem tantum incumbam, et varias methodos aperiam, quarum ope ex formulis traditis plures numeros amicabiles mihi elicere licuit. Quaelibet autem forma duplicem mihi suppeditavit methodum, prout factor communis a vel datus assumitur, vel ipse quaeritur; hasque methodos in sequentibus problematibus exponam.

§ 27. **Problema 1.** Invenire numeros amicabiles primae formae apq et ar, si factor communis a sit datus.

Solutio. Cum p, q et r sint numeri primi, atque $\int r = \int p . \int q$, seu $r + 1 = (p+1)(q+1)$, ponatur $p + 1 = x$ et $q + 1 = y$, fietque $r = xy - 1$, ideoque x et y ejusmodi esse oportet numeros, ut tam $x - 1$ et $y - 1$ quam $xy - 1$ sint numeri primi. Deinde ut $a(x-1)(y-1)$ et $a(xy-1)$ sint numeri amicabiles, oportet ut eorum aggregatum $a(2xy - x - y)$ aequale sit summae divisorum alterutrius $xy \int a$; unde nanciscimur hanc aequationem

$$xy \int a = 2axy - ax - ay, \quad \text{seu} \quad y = \frac{ax}{(2a - \int a)x - a}.$$

Sit brevitatis gratia $\frac{a}{2a - \int a} = \frac{b}{c}$, et $\frac{b}{c}$ sit valor fractionis $\frac{a}{2a - \int a}$ ad minimos terminos reductae, eritque $y = \frac{bx}{cx - b}$, seu $cy = \frac{bcx}{cx - b} = b + \frac{bb}{cx - b}$, unde habebimus $(cx - b)(cy - b) = bb$. Cum igitur $cx - b$ et $cy - b$ sint factores ipsius bb, quadratum cognitum bb in ejusmodi binos factores resolvi debet, quorum uterque numero b auctus fiat per c divisibilis, et quoti x et y inde emergentes ita sint comparati, ut $x - 1$, $y - 1$ et $xy - 1$ evadant numeri primi. Quae conditio quoties obtineri poterit, quod quidem pro quovis valore ipsius a assumto statim dispicitur, toties obtinebuntur numeri amicabiles, qui erunt

$$a(x-1)(y-1) \quad \text{et} \quad a(xy-1) \quad \text{Q. E. I.}$$

§ 28. **Coroll.** Prout igitur pro a alii aliique numeri accipiuntur, unde valores b et c innotescant, regulae emergent particulares, quarum ope numeri amicabiles, si qui in eo genere dantur, facile eruentur.

§ 29. **Regula 1.** Sit factor communis a potestas quaecunque binarii, puta $a = 2^n$, erit $\int a = 2^{n+1} - 1$, ideoque $2a - \int a = 1$, unde erit $\frac{a}{2a - \int a} = 2^n$, et propterea $b = 2^n$ et $c = 1$. Hinc oritur $(x - 2^n)(y - 2^n) = 2^{2n}$. Quare cum 2^{2n} alios non habeat factores nisi potestates binarii, erit

$$x-2^n=2^{n+k},\quad y-2^n=2^{n-k}$$

seu $$x=2^{n+k}+2^n;\quad y=2^{n-k}+2^n.$$

Quocirca dispiciendum est, an ejusmodi valor pro k detur, ut sequentes tres numeri

$$x-1=2^{n+k}+2^n-1$$
$$y-1=2^{n-k}+2^n-1$$
$$xy-1=2^{2n+1}+2^{2n+k}+2^{2n-k}-1$$

fiant numeri primi. Quod si succedat, erunt numeri amicabiles

$$2^n(2^{n+k}+2^n-1)(2^{n-k}+2^n-1)$$
$$2^n(2^{2n+1}+2^{2n+k}+2^{2n-k}-1).$$

Vel sit $n-k=m$, seu $n=m+k$, fietque

$$x-1=2^m(2^{2k}+2^k)-1=q$$
$$y-1=2^m(1+2^k)-1=p$$
$$xy-1=2^{2m}(2^{3k+1}+2^{3k}+2^k)-1=r$$

qui numeri, quoties fuerint primi, praebebunt numeros amicabiles.

§ 30. **Casus I.** Sit $k=1$, et numeri amicabiles obtinebuntur, quoties sequentes tres numeri fuerint primi

$$3.2^m-1;\quad 6.2^m-1;\quad 18.2^{2m}-1.$$

Tum enim positis

$$p=3.2^m-1;\quad q=6.2^m-1\quad\text{et}\quad r=18.2^{2m}-1$$

numeri amicabiles erunt $2^{m+1}pq$ et $2^{m+1}r$, ob $n=m+k=m+1$. Haecque est regula Cartesii a Schotenio tradita.

§ 31. *Exempl.* 1. Sit $m=1$, eritque

$p=3.2-1=5$ numerus primus

$q=6.2-1=11$ numerus primus

$r=18.4-1=71$ numerus primus.

Hinc ergo oriuntur numeri amicabiles:

$$2^2.5.11\ \text{et}\ 2^2.71\ \text{sive}\ 220\ \text{et}\ 284,$$

qui sunt minimi omnium, qui exhiberi possunt.

§ 32. *Exempl.* 2. Sit $m=2$, eritque $2^m=4$ et $2^{2m}=16$ atque

$p=3.4-1=11$ numerus primus

$q=6.4-1=23$ numerus primus

$r=18.16-1=287$ numerus non-primus

hincque adeo nulli numeri amicabiles oriuntur.

§ 33. *Exempl.* 3. Sit $m=3$, eritque $2^m=8$ et $2^{2m}=64$ atque

$p=3.8-1=23$ primus

$q=6.8-1=47$ primus

$r=18.64-1=1151$ primus.

Ergo hinc numeri amicabiles erunt

$$2^4.23.47 \text{ et } 2^4.1151, \text{ sive } 17296 \text{ et } 18416.$$

§ 34. *Exempla seqq.* Haec exempla cum sequentibus, in quibus exponenti m majores valores tribuuntur, commodius uno conspectu ita repraesentari poterunt:

Sit $m = 1$	2	3	4	5	6	7	8
erit $p = 5$	11	23	47	95*	191	383	767*
$q = 11$	23	47	95*	191	383	767*	1535*
$r = 71$	287*	1151	4607*	18431*	73727	294911	1179647

Ubi numeri non-primi asteriscis sunt notati, unde hinc tantum terni numeri amicabiles obtinentur, nempe

I. $\begin{cases} 2^2.5.7 \\ 2^2.71 \end{cases}$ II. $\begin{cases} 2^4.23.47 \\ 2^4.1151 \end{cases}$ III. $\begin{cases} 2^7.191.383 \\ 2^7.73727 \end{cases}$

Ulterius autem progredi non licet, quoniam valores ipsius r nimis fiunt magni, quam ut dignosci possit, utrum sint primi, nec ne? Tabulae namque numerorum primorum adhuc constructae vix ultra 100000 porriguntur.

§ 35. **Casus II.** Sit $k = 2$, et valores litterarum p, q, r, qui debent esse primi, erunt

$$p = 5.2^m - 1; \quad q = 20.2^m - 1; \quad r = 100.2^{2m} - 1,$$

quorum cum postremus semper sit per ternarium divisibilis, ob $2^{2m} = 3\alpha + 1$ et $r = 300\alpha + 99$, nulli numeri amicabiles consequuntur.

§ 36. **Casus III.** Ponatur $k = 3$, eritque

$$p = 9.2^m - 1; \quad q = 72.2^m - 1; \quad r = 648.2^{2m} - 1,$$

quorum cum nullus necessario videatur divisorem admittere, valores ipsorum p, q, r ex valoribus simplicioribus ipsius m oriundos hic conjunctim repraesentabo:

$m = 1$	2	3	4	5
$p = 17$	35*	71	143*	287*
$q = 143$*	287*	575*	1151	2303*
$r = 2591$	10367*	41471*	165887	663551

Hinc ergo, quoniam ulterius progredi non licet, nulli numeri amicabiles inveniuntur.

§ 37. **Casus IV.** Ponatur $k = 4$, et sequentes tres numeri debebunt esse primi

$$p = 17.2^m - 1; \quad q = 272.2^m - 1; \quad r = 4624.2^{2m} - 1.$$

Ubi cum r semper sit multiplum ternarii, patet hinc nullos prodire numeros amicabiles.

§ 38. **Casus V.** Ponatur $k = 5$, et sequentes tres numeri debebunt esse primi:

$$p = 33.2^m - 1; \quad q = 1056.2^m - 1; \quad r = 34848.2^{2m} - 1.$$

Ubi statim patet casum $m = 1$ esse inutilem, cum det $p = 65$. Sit ergo $m = 2$, fietque

$$p = 131; \quad q = 4223^*; \quad r = 557567;$$

ubi cum q non sit primus, et majores valores pro m ob defectum tabularum numerorum primorum examini subjici nequeant, neque hinc etiam novi numeri amicabiles eruuntur. At vero ob eandem rationem majores valores ipsi k tribuere non licet.

§ 39. **Scholion.** Quoniam potestates binarii pro a positae valorem ipsius c in fractione $\frac{b}{c}=\frac{a}{2a-\int a}$ unitati aequalem reddiderunt, hincque solutiones obtinere licuit, alios valores pro a, qui pariter ipsi c valorem $=1$ inducant, ponam. Inter hos autem imprimis sunt notandi, qui ex hac forma $a=2^n(2^{n+1}+e)$ nascuntur, siquidem $2^{n+1}+e$ sit numerus primus, tum enim fit $2a-\int a=e+1$, et $\frac{b}{c}=\frac{2^n(2^{n+1}+e)}{e+1}$: si igitur $e+1$ sit divisor numeratoris $2^n(2^{n+1}+e)$, valor ipsius c fiet itidem $=1$.

§ 40. **Regula 2.** Sit factor communis $a=2^n(2^{n+1}+2^k-1)$, at $2^{n+1}+2^k-1$ numerus primus, erit ob $e+1=2^k$, fractio

$$\frac{b}{c}=\frac{2^n(2^{n+1}+2^k-1)}{2^k}=2^{n-k}(2^{n+1}+2^k-1)$$

siquidem non sit $k>n$. Hac ergo hypothesi habebimus

$$b=2^{n-k}(2^{n+1}+2^k-1) \quad \text{et} \quad c=1.$$

Quadratum ergo bb in duos ejusmodi factores $(x-b)(y-b)$ resolvendum est, ex quibus non solum valores numerorum $x-1=p$ et $y-1=q$, sed etiam $xy-1=r$ fiant numeri primi. Cujusmodi casus si eruere liceat, erunt numeri amicabiles apq et ar. Verum hic notandum est eos casus rejiciendos esse, in quibus aliquis numerorum primorum p, q, r prodit divisor ipsius a, seu aequalis $2^{n+1}+2^k-1$, quia a per nullum alium numerum primum est divisibile.

Sit $n-k=m$, seu $n=m+k$, erit

$$a=2^{m+k}(2^{m+k+1}+2^k-1) \quad \text{et} \quad b=2^m(2^{m+k+1}+2^k-1).$$

Jam quia $2^{m+k+1}+2^k-1$ debet esse numerus primus, ponatur $2^{m+k+1}+2^k-1=f$, seu $f=2^k(2^{m+1}+1)-1$, ut sit $a=2^{m+k}f$ et $b=2^mf$, erit $bb=2^{2m}ff=(x-b)(y-b)$. Nunc ob f numerum primum, numerus $2^{2m}ff$ duplici modo in genere in duos factores resolvetur. Priori modo fiet $(x-b)(y-b)=2^{m-a}f.2^{m+a}f$, ideoque

$$\begin{aligned} x&=2^{m-a}f+2^mf, & p&=(2^{m-a}+2^m)f-1\\ y&=2^{m+a}f+2^mf, & q&=(2^{m+a}+2^m)f-1\\ && r&=(2^{2m+1}+2^{2m+a}+2^{2m-a})ff-1 \end{aligned}$$

qui tres numeri p, q, r debent esse primi. Posteriori modo resolutio fiet ita:

$$(x-b)(y-b)=2^{m\pm a}.2^{m\mp a}ff,$$

unde fit

$$\begin{aligned} x&=2^{m\pm a}+2^mf, & p&=2^{m\pm a}+2^mf-1\\ y&=2^{m\mp a}ff+2^mf, & q&=(2^{m\mp a}f+2^m)f-1\\ && r&=(2^{2m+1}f+2^{2m\pm a}+2^{2m\mp a}ff)f-1 \end{aligned}$$

et quoties p, q, r hoc modo prodeunt numeri primi, inde oriuntur numeri amicabiles apq et ar.

§ 41. **Casus I.** Sit $k = 1$, erit $a = 2^{m+1}(2^{m+2}+1)$; $b = 2^m(2^{m+2}+1)$ atque $f = 2^{m+2}+1$, qui numerus debet esse primus. Cum ergo sit $(x-b)(y-b) = 2^{2m} ff$, erit

vel	vel
$p = (2^{m-\alpha} + 2^m) f - 1$	$p = 2^{m\pm\alpha} + 2^m f - 1$
$q = (2^{m+\alpha} + 2^m) f - 1$	$q = (2^{m\mp\alpha} f + 2^m) f - 1$
$r = (2^{2m+1} + 2^{2m+\alpha} + 2^{2m-\alpha}) ff - 1$	$r = (2^{2m+1} f + 2^{2m\pm\alpha} + 2^{2m\mp\alpha} ff) f - 1.$

Notandum autem est, ut $2^{m+2}+1$ sit numerus primus, exponentem $m+2$ esse oportere potestatem binarii: valores ergo ipsius m erunt: 0, 2, 6, 14 etc. At casus $m = 0$ rejici debet, ob nullum valorem ipsius α assignabilem.

§ 42. *Exempl.* 1. Sit ergo $m = 2$, ut sit $a = 8.17$ et $b = 4.17 = 68$, atque $f = 17$. Cum igitur esse debeat $(x-b)(y-b) = 4^2.17^2$, erit resolutione in factores instituenda:

$x - 68 =$	2	4	8	34
$y - 68 =$	8.17^2	1156	578	136
$x =$	70	72	76	102
$y =$	2380	1224	646	204
$p =$	69*	71	75*	101
$q =$	2379*	1223	645*	203*
$r =$	166599*	88127*	49095*	20807

Hinc ergo nulli numeri amicabiles obtinentur.

§ 43. *Exempl.* 2. Sit $m = 6$, ut $a = 2^7.257$, $b = 2^6.257$, $f = 257$. Cum igitur sit

$$(x-b)(y-b) = 2^{12}.257^2,$$

resolutio ita institui debebit:

$x - 16448 =$	32.257
$y - 16448 =$	128.257
$x =$	24672
$y =$	49344
$p =$	24671
$q =$	49343*
$r =$	. . .

valores ex reliquis factoribus oriundi adhuc magis fiunt magni, quam ut, an primi sint nec ne, judicari possit.

§ 44. **Casus reliqui.** Cum $f = 2^{m+k+1} + 2^k - 1$ debeat esse numerus primus, quaeramus primo casus simpliciores, quibus hoc evenit, cum casus nimis compositos evolvere non liceat. Sit ergo $k = 2$, et ob $f = 2^{m+3} + 3$, valores idonei pro m erunt: 1, 3, 4. Sit $k = 3$, erit $f = 2^{m+4} + 7$, et valores idonei pro m erunt: 2, 4, 6. Casu $k = 4$, est $f = 2^{m+5} + 15$, et m erit 1, vel 3, neque ulterius progredi licet.

§ 45. *Exempl.* 1. Ponamus ergo $k = 2$ et $m = 1$, erit $f = 19$ et $a = 8.19$, atque $b = 2.19 = 38$, unde fiet $(x-38)(y-38) = 2^2.19^2 = 1444$, et resolutio dabit

$x - 38 =$	2	4	
$y - 38 =$	722	361	
$x =$	40		Neuter scilicet factor assumi potest impar.
$y =$	760	imp.	
$p =$	39*		

Quia hic jam p non est primus, patet hinc nullos numeros amicabiles resultare.

§ 46. *Exempl.* 2. Ponamus $k = 2$ et $m = 3$, ut sit $f = 67$, erit $a = 32.67$ et $b = 8.67 = 536$, unde fit $(x - 536)(y - 536) = 2^6.67^2$:

$x - 536 =$	268	16
$y - 536 =$	1072	17956
$x =$	804	552
$y =$	1608	...
$p =$	803*	1551*
$q =$	1607	...

Reliqui valores pro p praebent numeros per 3 divisibiles, quos propterea omisi. Sequentia exempla ad nimis magnos numeros deducunt.

§ 47. **Regula 3.** Sit ut ante $a = 2^n(2^{n+1} + 2^k - 1)$ et $2^{n+1} + 2^k - 1 = f$ numerus primus, at in fractione $\frac{b}{c} = \frac{2^n(2^{n+1} + 2^k - 1)}{2^k}$ sit $k > n$, eritque $b = 2^{n+1} + 2^k - 1$ et $c = 2^{k-n}$. Ponamus $k - n = m$, ut sit $k = m + n$, erit

$$a = 2^n(2^{n+1} + 2^{m+n} - 1), \quad b = 2^{n+1} + 2^{m+n} - 1 = f \text{ et } c = 2^m,$$

unde haec habebitur aequatio

$$(2^m x - b)(2^m y - b) = bb.$$

Cum autem $b = f$ sit numerus primus, alia resolutio locum non invenit praeter $1.bb$, ex qua fit

$$x = \frac{1+b}{2^m} \quad \text{et } y = \frac{b(1+b)}{2^m} \quad \text{sive}$$

$$x = 2^n + 2^{n+1-m} \quad \text{et } y = (2^{n+1} + 2^{m+n} - 1)(2^n + 2^{n+1-m})$$

Jam notandum est hos quatuor numeros esse oportere primos:

$$f = 2^{n+1} + 2^{m+n} - 1; \quad p = x - 1; \quad q = y - 1; \quad \text{et } r = xy - 1$$

atque necesse est ut sit $m < n + 1$. Quibus conditionibus si satisfiat, erunt numeri amicabiles: apq et ar.

§ 48. **Casus I.** Sit $m = 1$, erit $f = 2^{n+2} - 1$, $x = 2^{n+1}$ et $p = 2^{n+1} - 1$, fieri autem nequit, ut simul et f et p sit numerus primus, nisi casu $n = 1$, quo vero fit $q = 27$. Ergo ex hypothesi $m = 1$ nulli oriuntur numeri amicabiles.

§ 49. **Casus II.** Sit ergo $m = 2$, ut sit

$$f = 3.2^{n+1} - 1, \quad x = 3.2^{n-1} \quad \text{et } y = 3.2^{n-1}(3.2^{n+1} - 1), \quad \text{atque } a = 2^n f.$$

Sequentes ergo quatuor numeri debent esse primi:

$f = 3.2^{n+1} - 1$, $p = 3.2^{n-1} - 1$, $q = 3.2^{n-1}(3.2^{n+1} - 1) - 1$, et $r = 9.2^{2n-2}(3.2^{n+1} - 1) - 1$, unde formantur haec exempla:

$n=$	1	2	3	4	5
$f=$	11	23	47	95*	191
$p=$	2	5	11	...	47
$q=$	32*	137	563	...	9167*
$r=$	98*	827	6767*	...	...
		valet			

hincque ergo ex $n=2$ et $a=4.23$ nascuntur numeri amicabiles

$$\begin{cases} 4.23.5.137 \\ 4.23.827. \end{cases}$$

§ 50. **Casus ceteri.** Si $m=3$, iterum vel f vel p fit divisibile per 3, quod idem evenit si $m=5$, vel 7, etc. Sit ergo $m=4$, erit

$$f=9.2^{n+1}-1, \quad x=9.2^{n-3} \quad \text{et} \quad y=9.2^{n-3}(9.2^{n+1}-1), \quad \text{et} \quad a=2^n f,$$

unde formantur haec exempla:

$n=$	1	4	5	6
$f=$	35*	287*	575*	1151
$x=$	..	...	...	72
$y=$	..	...	...	82872
$p=$	..	...	...	71
$q=$	..	...	...	82871*
$r=$	..	...	...	...

Neque ergo hinc, neque ex majoribus valoribus ipsi m tribuendis numeros amicabiles elicere licet.

§ 51. **Regula 4.** Possunt etiam aliae expressiones pro factore communi a inveniri, ex quibus fractionis $\frac{b}{c}$ denominator c vel unitati, vel potestati binarii fiat aequalis. Fingamus namque $a=2^n(g-1)(h-1)$, ut sint $g-1$ et $h-1$ numeri primi; erit

$$\int a=(2^{n+1}-1)gh=2^{n+1}gh-gh;$$

at est $2a=2^{n+1}gh-2^{n+1}g-2^{n+1}h+2^{n+1}$, unde fit

$$2a-\int a=gh-2^{n+1}g-2^{n+1}h+2^{n+1}.$$

Ponatur $2a-\int a=d$, erit

$$gh-2^{n+1}(g+h)+2^{n+1}=d \quad \text{et} \quad (g-2^{n+1})(h-2^{n+1})=d-2^{n+1}+2^{2n+2};$$

unde per resolutionem in factores ejusmodi valores pro g et h elici debent, ut $g-1$ et $h-1$ fiant numeri primi; eritque tum $a=2^n(g-1)(h-1)$ et $\frac{b}{c}=\frac{a}{d}$.

I. Ponamus $n=1$, erit $(g-4)(h-4)=d+12$, ubi ut $d+12$ duos obtineat factores pares, sequentes prodibunt valores:

Sit $d=4$, erit $(g-4)(h-4)=16=2.8$, unde $g=6$, $h=12$, $a=2.5.11$, atque $\frac{b}{c}=\frac{2.5.11}{4}$, ergo $b=5.11$ et $c=2$.

Sit $d=8$, erit $(g-4)(h-4)=20=2.10$, unde $g=6$, $h=14$, $a=2.5.13$, atque $\frac{b}{c}=\frac{2.5.13}{8}$, ergo $b=5.13$ et $c=4$.

Sit $d=16$, erit $(g-4)(h-4)=28=2.14$, unde $g=6$, $h=18$, $a=2.5.17$, atque $\frac{b}{c}=\frac{2.5.17}{16}$, ergo $b=5.17$ et $c=8$.

II. Ponamus $n=2$, erit $(g-8)(h-8)=d+56$, atque $a=4(g-1)(h-1)$, unde sequentes casus resultant:

Sit $d=4$, erit $(g-8)(h-8)=60=6.10$, unde $g=14$ et $h=18$, $a=4.13.17$, atque $\frac{b}{c}=\frac{4.13.17}{4}$, ergo $b=13.17$ et $c=1$.

Sit $d=8$, erit $(g-8)(h-8)=64=4.16$, unde $g=12$ et $h=24$, $a=4.11.23$, atque $\frac{b}{c}=\frac{4.11.23}{8}$, ergo $b=11.23$ et $c=2$.

Sit $d=16$, erit $(g-8)(h-8)=72=6.12$, unde $g=14$ et $h=20$, $a=4.13.19$, atque $\frac{b}{c}=\frac{4.13.19}{16}$, ergo $b=13.19$ et $c=4$.

III. Ponamus $n=3$, ut sit $a=8(g-1)(h-1)$, oportebitque esse $(g-16)(h-16)=d+240$.

Sit $d=4$, erit $(g-16)(h-16)=244=2.122$, unde $g=18$, $h=138$, $a=8.17.137$, atque $\frac{b}{c}=\frac{8.17.137}{4}$, ergo $b=2.17.137$ et $c=1$.

Sit $d=8$, erit $(g-16)(h-16)=248=2.124$, unde $g=18$, $h=140$, $a=8.17.139$, atque $\frac{b}{c}=\frac{8.17.139}{8}$, ergo $b=17.139$ et $c=1$.

Sit $d=16$, erit $(g-16)(h-16)=256=4.64$, unde $g=20$, $h=80$, $a=8.19.79$; $\frac{b}{c}=\frac{8.19.79}{16}$, ergo $b=19.79$ et $c=2$.

Sit iterum $d=16$; $(g-16)(h-16)=8.32$, unde $g=24$ et $h=48$; $a=8.23.47$; $\frac{b}{c}=\frac{8.23.47}{16}$, ergo $b=23.47$ et $c=2$.

Sumtis autem hinc valoribus pro a, si numeri amicabiles statuantur $a(x-1)(y-1)$ et $a(xy-1)$, ut sint $x-1$, $y-1$, et $xy-1$ numeri primi, efficiendum est ut sit

$$(cx-b)(cy-b)=bb.$$

§ 52. *Exempl.* 1. Sit $a=2.5.11$, erit $b=5.11=55$ et $c=2$, unde fiet

$$(2x-55)(2y-55)=5^2.11^2$$

$2x-55=$	1	5	25	
$2y-55=$	3025	605	121	
$x=$	28	30	40	Hinc ergo nulli obtinentur numeri amicabiles.
$y=$	1540	330	88	
$x-1=$	27*	29	39*	
$y-1=$	..	329*	..	
$xy-1=$	..	..	..	

§ 53. *Exempl.* 2. Sit $a = 2.5.13$, erit $b = 5.13 = 65$ et $c = 4$, unde fit

$$(4x - 65)(4y - 65) = 5^2.13^2.$$

At hic numerus $5^2.13^2$ non resolvi potest in duos factores, qui 65 aucti fiant per 4 divisibiles: quod idem in valore $a = 2.5.17$ usu venit.

§ 54. *Exempl.* 3. Sit $a = 4.13.17$, erit $b = 13.17 = 221$ et $c = 1$ esseque oportet

$$(x - 221)(y - 221) = 13^2.17^2, \quad \text{unde}$$

$x - 221 =$	13	17	169
$y - 221 =$	3757	..	289
$x - 1 =$	233	237*	389
$y - 1 =$	3977*	...	509
$xy - 1 =$	...	...	198899

In resolutione ultima fit $x - 1$ et $y - 1$ numerus primus, quaestio ergo huc redit, utrum $xy - 1 = 198899$ sit numerus primus, nec ne? Etiamsi autem hic numerus terminum 100000 excedat, tamen demonstrare possum eum esse primum, unde numeri amicabiles erunt:

$$\begin{cases} 4.13.17.389.509 \\ 4.13.17.198899. \end{cases}$$

§ 55. **Scholion.** Numerum autem hunc 198899 esse primum inde colligo, quod observavi esse $198899 = 2.47^2 + 441^2$, ita ut 198899 sit numerus in hac forma $2aa + bb$ contentus. Certum autem est, si quis numerus unico modo in forma $2aa + bb$ contineatur, tum eum esse primum, sin autem duplici vel pluribus modis ad formam $2aa + bb$ redigi queat, tum esse compositum. Quaesivi ergo utrum a numero hoc 198899 aliud quadratum duplum praeter 47^2 subtrahi queat, ut residuum evadat quadratum, nullumque subducto calculo inveni: ex quo tuto conclusi hunc numerum esse primum, ideoque numeros inventos esse amicabiles. Ex reliquis autem valoribus ipsius a, quos exhibui, nulli reperiuntur numeri amicabiles.

§ 56. **Regula 5.** Possunt etiam alii numeri idonei pro a assumi, ex quibus numeros amicabiles eruere liceat. Cum autem pro iis regula generalis tradi nequeat, aliquos tantum hic evolvam, ad quorum imitationem non erit difficile alios excogitare.

I. Sit ergo $a = 3^2.5.13$, erit $\int a = 13.6.14$, et ob $2a = 90.13$ et $\int a = 84.13$, erit $2a - \int a = 6.13$, atque $\frac{b}{c} = \frac{a}{2a - \int a} = \frac{3^2.5.13}{6.13} = \frac{15}{2}$, ideoque $b = 15$ et $c = 2$.

II. Sit $a = 3^2.7.13$, erit $\int a = 13.8.14 = 16.7.13$, unde ob $2a = 18.7.13$, erit $2a - \int a = 2.7.13$, ideoque $\frac{b}{c} = \frac{3^2.7.13}{2.7.13} = \frac{9}{2}$, unde $b = 9$ et $c = 2$.

III. Sit $a = 3^2.7^2.13$, erit $\int a = 13.3.19.14 = 2.3.7.13.19$, et $2a = 42.3.7.13$, unde $2a - \int a = 4.3.7.13$, ideoque $\frac{b}{c} = \frac{3^2.7^2.13}{4.3.7.13} = \frac{21}{4}$, ergo $b = 21$ et $c = 4$.

IV. Sit $a = 3^3.5$, erit $\int a = 5.8.6 = 16.3.5$. Ergo ob $2a = 18.3.5$, erit $2a - \int a = 2.3.5$, hincque $\frac{b}{c} = \frac{3^3.5}{2.3.5} = \frac{9}{2}$, et $b = 9$ et $c = 2$.

V. Sit $a = 3^2.5.13.19$, erit $\int a = 13.6.14.20 = 16.3.5.7.13$, et ob $2a = 114.3.5.13$ et $\int a = 112.3.5.13$, erit $\frac{b}{c} = \frac{3^2.5.13.19}{2.3.5.13} = \frac{3.19}{2}$ et $b = 3.19 = 57$ et $c = 2$.

VI. Sit $a = 3^2.7^2.13.19$, erit $\int a = 13.3.19.14.20 = 8.3.5.7.13.19$ et ob $2a = 42.3.7.13.19$ erit $\frac{b}{c} = \frac{3^2.7^2.13.19}{2.3.7.13.19} = \frac{21}{2}$, unde fit $b = 21$ et $c = 2$.

Positis autem numeris amicabilibus $a(x-1)(y-1)$ et $a(xy-1)$, fieri debet

$$(cx - b)(cy - b) = bb.$$

§ 57. *Exempl.* 1. Sit $b = 15$, $c = 2$, erit $a = 3^2.5.13$ et satisfieri oportet huic aequationi

$$(2x - 15)(2y - 15) = 225:$$

$2x - 15 =$	1	5	9
$2y - 15 =$	225	45	25
$x =$	8	10	12
$y =$	120	30	20
$x - 1 =$	7	9*	11
$y - 1 =$	119*	..	19
$xy - 1 =$	..	..	239

Numeri ergo amicabiles sunt $\begin{cases} 3^2.5.13.11.19 \\ 3^2.5.13.239. \end{cases}$

§ 58. *Exempl.* 2. Sit $b = 9$, $c = 2$, erit vel $a = 3^2.7.13$, vel $a = 3^4.5$, et aequatio resolvenda $(2x - 9)(2y - 9) = 81$.

$2x - 9 =$	3
$2y - 9 =$	27
$x =$	6
$y =$	18
$x - 1 =$	5
$y - 1 =$	17
$xy - 1 =$	107

Unde cum sit $x - 1 = 5$, hic valor cum $a = 3^4.5$ combinari nequit. Erunt ergo numeri amicabiles:

$\begin{cases} 3^2.7.13.5.17 \\ 3^2.7.13.107. \end{cases}$

§ 59. *Exempl.* 3. Sit $b = 21$ et $c = 4$, erit $a = 3^2.7^2.13$ et aequatio resolvenda

$$(4x - 21)(4y - 21) = 441.$$

$4x - 21 =$	3
$4y - 21 =$	147
$x =$	6
$y =$	42
$x - 1 =$	5
$y - 1 =$	41
$xy - 1 =$	251

Quia x et y debent esse numeri pares, alia resolutio locum non habet. Ex hac ergo prodeunt numeri amicabiles hi:

$\begin{cases} 3^2.7^2.13.5.41 \\ 3^2.7^2.13.251 \end{cases}$

§ 60. *Exempl.* 4. Sit $b=21$ et $c=2$, erit $a=3^2.7^2.13.19$ et aequatio resolvenda

$$(2x-21)(2y-21)=441.$$

$2x-21=$	3	7
$2y-21=$	147	63
$x=$	12	14
$y=$	84	42
$x-1=$	11	13
$y-1=$	83	41
$xy-1=$	1007*	587

Quia autem valor $x-1=13$ jam in valore a continetur, hinc nulli obtinentur numeri amicabiles.

§ 61. *Exempl.* 5. Sit $b=57$ et $c=2$, erit $a=3.5.13.19$ et aequatio resolvenda

$$(2x-57)(2y-57)=3249.$$

$2x-57=$	3	19
$2y-57=$	1083	171
$x=$	30	38
$y=$	570	114
$x-1=$	29	37
$y-1=$	569	113
$xy-1=$	17099	4331*

Hinc ergo oriuntur numeri amicabiles hi:

$$\begin{cases} 3^2.5.13.19.29.569 \\ 3^2.5.13.19.17099. \end{cases}$$

§ 62. *Exempl.* 6. Sit $b=45$ et $c=2$, erit $a=3^4.5.11$, et aequatio resolvenda

$$(2x-45)(2y-45)=2025.$$

$2x-45=$	3	15
$2y-45=$	675	135
$x=$	24	30
$y=$	360	90
$x-1=$	23	29
$y-1=$	359	89
$xy-1=$	8639*	2699

Hinc ergo oriuntur numeri amicabiles:

$$\begin{cases} 3^4.5.11.29.89 \\ 3^4.5.11.2699. \end{cases}$$

§ 63. *Exempl.* 7. Sit $b=77$ et $c=2$, erit $a=3^2.7^2.11.13$ et aequatio resolvenda

$$(2x-77)(2y-77)=49.121.$$

$2x-77=$	7	11
$2y-77=$	847	539
$x=$	42	44
$y=$	462	308
$x-1=$	41	43
$y-1=$	461	307
$xy-1=$	19403	13551*

Hinc ergo oriuntur numeri amicabiles:

$$\begin{cases} 3^2.7^2.11.13.41.461 \\ 3^2.7^2.11.13.19403. \end{cases}$$

§ 64. *Exempl.* 8. Sit $b = 105$, $c = 2$, erit $a = 3^2.5.7$ et aequatio resolvenda

$$(2x - 105)(2y - 105) = 105^2.$$

$2x - 105 =$	3	7	15	35
$2y - 105 =$	3675	..	735	..
$x =$	54	56	60	70
$y =$	1890	..	420	..
$x - 1 =$	53	55*	59	69*
$y - 1 =$	1889	..	419	
$xy - 1 =$	102059	..	25199*	

Cum 102059 sit numerus primus, quia continetur in forma $8a + 3$ et unico modo ad formam $2aa + bb$ reducitur, numeri amicabiles hinc orti erunt:

$$\begin{cases} 3^2.5.7.53.1889 \\ 3^2.5.7.102059. \end{cases}$$

§ 65. **Scholion.** Numeri ergo amicabiles, quos hactenus ex forma apq, ar invenimus, sunt:

I.	$2^2.5.11$ / $2^2.71$	V.	$4.13.17.389.509$ / $4.13.17.198899$	IX.	$3^2.5.13.19.29.569$ / $3^2.5.13.19.17099$
II.	$2^4.23.47$ / $2^4.1151$	VI.	$3^2.5.13.11.19$ / $3^2.5.13.239$	X.	$3^4.5.11.29.89$ / $3^4.5.11.2699$
III.	$2^7.191.393$ / $2^7.73727$	VII.	$3^2.7.13.5.17$ / $3^2.7.13.107$	XI.	$3^2.7^2.11.13.41.461$ / $3^2.7^2.11.13.19403$
IV.	$4.23.5.137$ / $4.23.827$	VIII.	$3^2.7^2.13.5.41$ / $3^2.7^2.13.251$	XII.	$3^2.5.7.53.1889$ / $3^2.5.7.102059$

§ 66. **Problema 2.** Invenire numeros amicabiles secundae formae apq, ars, positis p, q, r, s numeris primis et factore communi a dato.

Solutio. Cum factor communis a detur, quaeratur ex eo valor fractionis $\frac{b}{c} = \frac{a}{2a - \int a}$ in minimis terminis, hincque erit $a : \int a = b : 2b - c$. Deinde cum esse debeat $\int p . \int q = \int r . \int s$ seu $(p+1)(q+1) = (r+1)(s+1)$, ponatur uterque valor $= \alpha\beta xy$, et sumatur: $p = \alpha x - 1$, $q = \beta y - 1$, $r = \beta x - 1$, $s = \alpha y - 1$, ubi manifestum est hos numeros α, β, x, y ejusmodi esse debere, ut p, q, r, s fiant numeri primi, et numeri amicabiles erunt:

$$a(\alpha x - 1)(\beta y - 1) \quad \text{et} \quad a(\beta x - 1)(\alpha y - 1).$$

Praeterea vero ex natura numerorum amicabilium esse debet:

$$\alpha\beta xy \int a = a(\alpha x - 1)(\beta y - 1) + a(\beta x - 1)(\alpha y - 1)$$

seu ob $\int a : a = 2b - c : b$, erit

$$\left.\begin{matrix} 2b\alpha\beta xy \\ - c\alpha\beta xy \end{matrix}\right\} = \left\{\begin{matrix} 2b\alpha\beta xy - b\alpha x - b\beta y + 2b \\ - b\beta x - b\alpha y \end{matrix}\right.$$

vel $c\alpha\beta xy = b(\alpha + \beta)(x + y) - 2b$. Unde fit

$$c^2\alpha^2\beta^2 xy - bc\alpha\beta(\alpha + \beta)x + bb(\alpha + \beta)^2 = -2bc\alpha\beta + bb(\alpha + \beta)^2$$
$$- bc\alpha\beta(\alpha + \beta)y$$

quare satisfieri debet huic aequationi:

$$(c\alpha\beta x - b(\alpha + \beta))(c\alpha\beta y - b(\alpha + \beta)) = bb(\alpha + \beta)^2 - 2bc\alpha\beta.$$

Numerus ergo $bb(\alpha+\beta)^2 - 2bc\alpha\beta$ quovis casu in duos ejusmodi factores, qui sint P, Q resolvi debet, ut positis

$$x = \frac{P + b(\alpha+\beta)}{c\alpha\beta} \quad \text{et} \quad y = \frac{Q + b(\alpha+\beta)}{c\alpha\beta}$$

hi numeri x et y non solum fiant integri, sed etiam $\alpha x - 1$, $\beta y - 1$, $\beta x - 1$, et $\alpha y - 1$ numeri primi. Erit igitur

$$p = \frac{P + b\alpha + (b-c)\beta}{c\beta}, \quad q = \frac{Q + b\beta + (b-c)\alpha}{c\alpha}, \quad r = \frac{P + b\beta + (b-c)\alpha}{c\beta}, \quad s = \frac{Q + b\alpha + (b-c)\beta}{c\alpha}.$$

Quovis ergo valore ipsius a proposito, unde reperitur $\frac{b}{c} = \frac{a}{2a - \int a}$, dispiciendum est, utrum cum numeri α et β ita assumi, tum resolutio haec

$$bb(\alpha+\beta)^2 - 2bc\alpha\beta = PQ$$

ita institui queat, ut valores modo traditi pro p, q, r et s fiant numeri primi, et tales quidem, ut factor communis a nullum eorum involvat. Quoties autem his conditionibus satisfieri poterit, erunt numeri amicabiles: apq et ars.

§ 67. **Coroll.** Quoniam esse nequit $\alpha = \beta$, pro his numeris α et β ponantur numeri simpliciores, hincque orientur casus sequentes:

I. Sit $\alpha = 1$, $\beta = 2$, erit $PQ = 9bb - 4bc$ et

$$p = \frac{P+3b-2c}{2c}, \quad q = \frac{Q+3b-c}{c}, \quad r = \frac{P+3b-c}{c}, \quad s = \frac{Q+3b-2c}{2c}.$$

II. Sit $\alpha = 1$, $\beta = 3$, erit $PQ = 16bb - 6bc$ et

$$p = \frac{P+4b-3c}{3c}, \quad q = \frac{Q+4b-c}{c}, \quad r = \frac{P+4b-c}{c}, \quad s = \frac{Q+4b-3c}{3c}.$$

III. Sit $\alpha = 2$, $\beta = 3$, erit $PQ = 25bb - 12bc$ et

$$p = \frac{P+5b}{3c} - 1, \quad q = \frac{Q+5b}{2c} - 1, \quad r = \frac{P+5b}{2c} - 1, \quad s = \frac{Q+5b}{3c} - 1.$$

IV. Sit $\alpha = 1$, $\beta = 4$, erit $PQ = 25bb - 8bc$ et

$$p = \frac{P+5b}{4c} - 1, \quad q = \frac{Q+5b}{c} - 1, \quad r = \frac{P+5b}{c} - 1, \quad s = \frac{Q+5b}{4c} - 1.$$

V. Sit $\alpha = 3$, $\beta = 4$, erit $PQ = 49bb - 24bc$ et

$$p = \frac{P+7b}{4c} - 1, \quad q = \frac{Q+7b}{3c} - 1, \quad r = \frac{P+7b}{3c} - 1, \quad s = \frac{Q+7b}{4c} - 1.$$

VI. Sit $\alpha = 1$, $\beta = 5$, erit $PQ = 36bb - 10bc$ et

$$p = \frac{P+6b}{5c} - 1, \quad q = \frac{Q+6b}{c} - 1, \quad r = \frac{P+6b}{c} - 1, \quad s = \frac{Q+6b}{5c} - 1.$$

VII. Sit $\alpha = 2$, $\beta = 5$, erit $PQ = 49bb - 20bc$ et

$$p = \frac{P+7b}{5c} - 1, \quad q = \frac{Q+7b}{2c} - 1, \quad r = \frac{P+7b}{2c} - 1, \quad s = \frac{Q+7b}{5c} - 1.$$

VIII. Sit $\alpha = 3$, $\beta = 5$, erit $PQ = 64bb - 30bc$ et

$$p = \frac{P+8b}{5c} - 1, \quad q = \frac{Q+8b}{3c} - 1, \quad r = \frac{P+8b}{3c} - 1, \quad s = \frac{Q+8b}{5c} - 1,$$

IX. Sit $\alpha = 4$, $\beta = 5$, erit $PQ = 81bb - 40bc$ et

$$p = \frac{P+9b}{5c} - 1, \quad q = \frac{Q+9b}{4c} - 1, \quad r = \frac{P+9b}{4c} - 1, \quad s = \frac{Q+9b}{5c} - 1.$$

X. Sit $\alpha = 1$, $\beta = 6$, erit $PQ = 49bb - 12bc$ et

$$p = \frac{P+7b}{6c} - 1, \quad q = \frac{Q+7b}{c} - 1, \quad r = \frac{P+7b}{c} - 1, \quad s = \frac{Q+7b}{6c} - 1.$$

XI. Sit $\alpha = 5$, $\beta = 6$, erit $PQ = 121bb - 60bc$ et

$$p = \frac{P+11b}{6c} - 1, \quad q = \frac{Q+11b}{5c} - 1, \quad r = \frac{P+11b}{5c} - 1, \quad s = \frac{Q+11b}{6c} - 1.$$

Secundum hos igitur casus valores ipsius a jam ante adhibitos, quia prae ceteris ad numeros amicabiles inveniendos videntur apti, evolvam, ex iis autem potissimum eos eligam, qui actu ad numeros amicabiles deducunt.

§ 68. *Exempl.* 1. Sit $a = 2^2$, erit $b = 4$ et $c = 1$. Sumatur casus secundus quo $\alpha = 1$, $\beta = 3$, ut numeri amicabiles sint 2^2pq et 2^2rs, fierique debet

$$PQ = 16.16 - 6.4 = 232, \quad \text{atque}$$

$$p = \frac{P+16}{3} - 1, \quad q = Q + 16 - 1, \quad r = P + 16 - 1, \quad s = \frac{Q+16}{3} - 1$$

factores ergo numeri 232 ita debent esse comparati, ut 16 aucti, fiant per 3 divisibiles:

$P = 2$	Alia resolutio nulla succedit; si enim poneretur $P = 8$, fieret Q numerus impar, neque ergo q et s numeri primi esse possent. Hinc ergo obtinentur hi numeri amicabiles:
$Q = 116$	
$P + 16 = 18$	
$Q + 16 = 132$	
$p = 5$	
$q = 131$	$\begin{cases} 2^2.\,5.\,131 \\ 2^2.\,17.\,43. \end{cases}$
$r = 17$	
$s = 43$	

§ 69. *Exempl.* 2. Si $\alpha = 1$ et $\beta = 3$, et a potestas binarii altior, inventio numerorum amicabilium non succedit, donec perveniatur ad $a = 2^8$. Tum autem erit $b = 2^8$ et $c = 1$, atque

$$PQ = 16.2^{16} - 6.2^8 = 2^9(2^{11} - 3) = 512.2045 = 512.5.409$$

$$p = \frac{P+1024}{3} - 1, \quad q = Q + 1024 - 1, \quad r = P + 1024 - 1, \quad s = \frac{Q+1024}{3} - 1$$

unde factores P et Q ita debent esse comparati, ut quaternario aucti per 3, vel, ut quoti fiant pares, per 6 sint divisibiles.

$P =$	2	8	20	32	80	128	320	1280
$Q =$	..				13088	8180		
$P + 1024 =$	1026	1032	1044	1056	1104	1152	1344	2304
$Q + 1024 =$	..	..			14112	9204		
$p =$	341	343*	347		367	383	447*	767*
$q =$	..	..			14111*	9203		
$r =$	1025*	..	1043*	1055*	1103	1151	1343	2303
$s =$	..	..	..	..	4703	3067		

Erunt ergo numeri amicabiles $\begin{cases} 2^8.\,383.\,9203 \\ 2^8.\,1151.\,3067. \end{cases}$

§ 70. *Exempl.* 3. Sit $\alpha = 2$ et $\beta = 3$, et sumatur $a = 3^2.\,5.\,13$, ut sit $b = 15$ et $c = 2$; erit $PQ = 25.225 - 12.30 = 3^4.5.13$;

$$p = \frac{P+75}{6} - 1,\quad q = \frac{Q+75}{4} - 1,\quad r = \frac{P+75}{4} - 1,\quad s = \frac{Q+75}{6} - 1,$$

unde factores P, Q ejusmodi esse debent, ut ternario aucti fiant per 24 divisibiles.

$P =$	45
$Q =$	117
$P + 75 =$	120
$Q + 75 =$	192
$p =$	19
$q =$	47
$r =$	29
$s =$	31

Aliae resolutiones non inveniunt locum; unde hinc numeri amicabiles prodeunt:

$\begin{cases} 3^2.\,5.\,13.\,19.\,47 \\ 3^2.\,5.\,13.\,29.\,31. \end{cases}$

§ 71. *Exempl.* 4. Sit $\alpha = 1$ et $\beta = 4$; sumatur $a = 3^2.\,5$, ut sit $b = 9$, $c = 2$, erit

$$PQ = 25.81 - 8.18 = 9.11.19 \quad \text{et}$$

$$p = \frac{P+45}{8} - 1,\quad q = \frac{Q+45}{2} - 1,\quad r = \frac{P+45}{2} - 1,\quad s = \frac{Q+45}{8} - 1$$

unde P et Q ejusmodi esse debent numeri, ut quinario aucti per 8 fiant divisibiles.

$P =$	3	19
$Q =$	627	99
$P + 45 =$	48	64
$Q + 45 =$	672	144
$p =$	5	7
$q =$	335*	71
$r =$	23	31
$s =$	83	17

Hinc ergo oriuntur numeri amicabiles

$\begin{cases} 3^2.\,5.\,7.\,71 \\ 3^2.\,5.\,31.\,17. \end{cases}$

§ 72. **Scholion.** Hae autem operationes nimis sunt incertae, ac plerumque plures frustra instituuntur, antequam numeri amicabiles se offerunt. Labor quoque foret vehementer prolixus, si singulis valoribus ipsius a, quos quidem supra exhibui, per singulos casus litterarum α et β percurrere velimus, atque nimis raro evenit, ut quatuor numeri pro p, q, r et s resultantes simul fiant primi. Tum vero etiam inventio numerorum amicabilium per determinationem rationis α et β nimis restringitur, atque dantur casus hujusmodi numerorum, in quibus ratio α et β tam est complicata, ut nulla probabili ratione eligi potuisset, cujusmodi sunt numeri amicabiles $2^4.19.8563$ et $2^4.83.2039$, ad quos hac via inveniendos ratio $\alpha:\beta$ assumi debuisset $5:21$ vel $1:102$. Hanc ob rem huic methodo nimis sterili et operosae diutius non immoror, sed aliam viam aperiam, qua facilius et expeditius numeros amicabiles tam hujus secundae formae, quam aliarum magis compositarum investigare liceat, et quae similis sit praecedenti, quae tribus tantum numeris primis reperiendis absolvitur.

§ 73. **Problema 3.** Invenire numeros amicabiles hujus formae apq et afr, ubi p, q et r sint numeri primi, f sive primus sive compositus, qui perinde ac factor communis a sit datus.

Solutio. Quaerantur iterum ex cognito factore communi a valores b et c, ut sit $\frac{b}{c} = \frac{a}{2a - \int a}$, et sit numeri f summa divisorum $\int f = gh$. Cum igitur primo requiratur ut sit

$$\int p . \int q = \int f . \int r, \quad \text{erit} \quad (p+1)(q+1) = gh(r+1).$$

Ponatur $r + 1 = xy$, $p + 1 = hx$ et $q + 1 = gy$, et necesse erit, ut sint hi tres numeri primi, scilicet $p = hx - 1$, $q = gy - 1$ et $r = xy - 1$. Deinde opus est, ut sit

$$\int apq = ghxy \int a = a(hx-1)(gy-1) + af(xy-1) = a((gh+f)xy - hx - gy + 1 - f),$$

$$\text{seu} \quad 2bghxy - cghxy = b(gh+f)xy - bhx - bgy + b(1-f), \quad \text{vel}$$

$$(bf - bgh + cgh)xy - bhx - bgy = b(f-1).$$

Ponamus brevitatis gratia $bf - bgh + cgh = e$, erit

$$eexy - ebhx - ebgy = eb(f-1) \quad \text{sive}$$

$$(ex - bg)(ey - bh) = bbgh + be(f-1).$$

Numerus ergo $bbgh + be(f-1)$ in duos ejusmodi factores, qui sint P et Q, resolvi debet, ut fiant $x = \frac{P + bg}{e}$ et $y = \frac{Q + bh}{e}$ numeri integri, tum vero $hx - 1$; $gy - 1$ et $xy - 1$ numeri primi. Quae conditio, quoties impleri poterit, erunt numeri amicabiles

$$\begin{cases} a(hx-1)(gy-1) \\ af(xy-1). \end{cases}$$

Notandum est, neque ullum horum numerorum primorum $hx - 1$, $gy - 1$, $xy - 1$, neque ullum factorem ipsius f divisorem esse debere ipsius a; nec non f et $xy - 1$ esse debere numeros primos inter se.

§ 74. **Coroll. 1.** Si f sit numerus primus, uti secunda forma numerorum amicabilium postulat, erit $f + 1 = gh$ et propterea $f = gh - 1$. Hoc ergo casu erit

$$e = cgh - b \quad \text{et} \quad PQ = bbgh + be(gh-2) \quad \text{seu}$$

$$PQ = bcgghh - 2bcgh + 2bb.$$

Unde quaeri debent numeri x et y supra memoratis proprietatibus praediti, ut sit

$$x = \frac{P + bg}{e} \quad \text{et} \quad y = \frac{Q + bh}{e}.$$

§ 75. **Coroll. 2.** His igitur formulis ita uti conveniet, ut pro a successive alii atque alii valores ex iis, quos supra exposui, substituantur, atque pro singulis litterae f varii numeri tam primi quam compositi substituantur, qui quidem ad numeros amicabiles inveniendos idonei videantur.

§ 76. **Casus I.** Sit $a = 4$ (ex valore enim $a = 2$ nullos obtineri numeros amicabiles observavi), eritque $b = 4$ et $c = 1$. Tum positis numeris amicabilibus $4pq$ et $4fr$, sit $ff = gh$ et $e = 4f - 3gh$. Deinde per resolutionem quaerantur factores P et Q, ut sit $PQ = 16gh + 4e(f-1)$. Hineque eruantur numeri integri x et y, ut sit

$$x = \frac{P + 4g}{e} \quad \text{et} \quad y = \frac{Q + 4h}{e}$$

et ex his deriventur valores litterarum $p = hx - 1$, $q = gy - 1$ et $r = xy - 1$, qui si fuerint numeri primi, erunt $4pq$ et $4fr$ numeri amicabiles.

§ 77. *Exempl.* 1. Sit $f = 3$, erit $ff = gh = 4$, hincque $e = 12 - 12 = 0$, unde patet ex hac hypothesi nihil obtineri.

§ 78. *Exempl.* 2. Sit $f = 5$, erit $ff = gh = 6$, $e = 20 - 18 = 2$, atque

$$PQ = 16.6 + 8.4 = 128.$$

Jam ex $gh = 6$ ponatur primo $g = 2$ et $h = 3$ fietque

$$x = \frac{P + 8}{2} \quad \text{et} \quad y = \frac{Q + 12}{2}.$$

Quare sequentes habebuntur resolutiones:

$P =$	2	4	8	16	32	64
$Q =$	64	32	16	8	4	2
$x =$	5	6	8	12	20	36
$y =$	38	22	14	10	8	7
$p = 3x - 1 =$	14*	17	23	35*	59	107
$q = 2y - 1 =$	..	43	27*	19	15*	13
$r = xy - 1 =$	..	131	111*	119*	159	251

Hinc ergo prodeunt numeri amicabiles:

$$\begin{cases} 4.17.43 \\ 4.5.131 \end{cases} \quad \text{et} \quad \begin{cases} 4.13.107 \\ 4.5.251. \end{cases}$$

Ponatur secundo $g = 1$, $h = 6$, fietque: $x = \frac{P + 4}{2}$ et $y = \frac{Q + 24}{2}$.

$P =$	2	4	8	16	32	64
$Q =$	64	32	16	8	4	2
$x =$	3	4	6	10	18	34
$y =$	44	28	20	16	14	13
$p = 6x - 1 =$	17	23	35*	59	107	203*
$q = 1y - 1 =$	43	27*	19	15*	13	12*
$r = xy - 1 =$	131	111*	119*	159	251	441*

Iidem ergo prodeunt bini numeri amicabiles, qui ante; scilicet

$$\begin{cases} 4.17.43 \\ 4.5.131 \end{cases} \quad \text{et} \quad \begin{cases} 4.13.107 \\ 4.5.251. \end{cases}$$

§ 79. *Exempl.* 3. Sit $f = 7$, erit $\int f = gh = 8$, $e = 28 - 24 = 4$ et $PQ = 16.8 + 16.6 = 224$. Sit ergo primo $g = 2$, $h = 4$ erit

$$x = \frac{P+8}{4}, \quad y = \frac{Q+16}{4}, \quad p = 4x - 1, \quad q = 2y - 1, \quad r = xy - 1.$$

$P =$	4	8	28	56
$Q =$	56	28	8	4
$x =$	3	4	9	16
$y =$	18	11	6	5
$p =$	11	15*	35*	63*
$q =$	35*	21*	11	9*
$r =$	53	43	53	79

Hinc ergo nulli prodeunt numeri amicabiles.

Sit secundo

$$g = 1, \quad h = 8, \text{ erit } x = \frac{P+4}{4} \text{ et } y = \frac{Q+32}{4} \text{ et } p = 8x - 1, \quad q = y - 1, \quad r = xy - 1$$

$P =$	4	8	28	56
$Q =$	56	28	8	4
$x =$	2	3	8	15
$y =$	22	15	10	9
$p =$	15*	23	63*	119*
$q =$	21*	14*	9*	8*
$r =$	43	44*	79	134*

Ut ante.

§ 80. *Exempl.* 4. Sit $f = 11$, erit $gh = 12$, $e = 8$, $PQ = 16.12 + 32.10 = 512$, vel erit $(8x - 4g)(8y - 4h) = 512$, quae aequatio deprimitur ad $(2x - g)(2y - h) = 32$, qua resoluta erit $p = hx - 1$, $q = gy - 1$ et $r = xy - 1$. Sive autem hic ponatur $g = 1$, $h = 12$; sive $g = 2$, $h = 6$, sive $g = 3$, $h = 4$, nulli prodeunt numeri primi pro p, q et r.

§ 81. *Exempl.* 5. Sit $f = 13$, erit $gh = 14$, $e = 10$, $PQ = 224 + 40.12 = 704$ et $(10x - 4g)(10y - 4h) = 704$, quae deprimitur ad $(5x - 2g)(5y - 2h) = 176$. Hinc autem nulli alii numeri amicabiles obtinentur nisi

$$\begin{cases} 4.\ 5.\ 251 \\ 4.\ 13.\ 107 \end{cases}$$

qui jam ante (§ 78) sunt inventi. Simul vero jam patet, etiamsi pro f majores numeri primi statuantur, nullos novos numeros amicabiles prodire, quoniam vel p vel q sortietur valorem minorem, qui pro f assumi potuisset.

§ 82. *Exempl.* 6. Sit $f = 5.13$, erit $gh = 6.14 = 84$, $e = 8$, $PQ = 16.84 + 32.64 = 64.53$, et $(8x - 4g)(8y - 4h) = 64.53$, seu $(2x - g)(2y - h) = 4.53$. Hincque invenietur in numeris primis: $p = 43$, $q = 2267$ et $r = 1187$, unde erunt numeri amicabiles:

$$\begin{cases} 4.\ 43.\ 2267 \\ 4.\ 5.\ 13.\ 1187. \end{cases}$$

§ 83. **Casus II.** Sit $a = 2^3 = 8$, erit $b = 8$, $c = 1$; tum positis numeris amicabilibus $8pq$ et $8fr$, et $ff = gh$, erit $e = 8f - 7gh$, atque

$$(ex - 8g)(ey - 8h) = 64gh + 8e(f - 1)$$

unde casus sunt dignoscendi, quibus fiunt numeri primi

$$p = hx - 1,\ q = gy - 1 \text{ et } r = xy - 1.$$

§ 84. *Exempl.* 1. Sit $f = 11$, erit $gh = 12$, $e = 4$, atque

$$(4x - 8g)(4y - 8h) = 64.12 + 32.10 = 64.17, \quad \text{seu} \quad (x - 2g)(y - 2h) = 4.17 = 68.$$

Hinc autem nulli numeri amicabiles reperiuntur.

§ 85. *Exempl.* 2. Sit $f = 13$, erit $gh = 14$, $e = 6$ atque

$$(6x - 8g)(6y - 8h) = 64.14 + 48.12 = 64.23, \quad \text{seu} \quad (3x - 4g)(3y - 4h) = 16.23;$$

verum etiam haec hypothesis est inutilis.

§ 86. *Exempl.* 3. Sit $f = 17$, erit $gh = 18$, $e = 10$, atque

$$(10x - 8g)(10y - 8h) = 64.18 + 80.16 = 64.38, \quad \text{seu} \quad (5x - 4g)(5y - 4h) = 32.19,$$

hincque prodeunt numeri amicabiles:

$$\begin{cases} 8.\ 23.\ 59 \\ 8.\ 17.\ 79. \end{cases}$$

§ 87. *Exempl.* 4. Magis foecunda est hypothesis $f = 11.23$, minor enim valor pro f in compositis substitui nequit; erit $gh = 12.24$, $e = 8$, unde

$$(8x - 8g)(8y - 8h) = 64.12.24 + 64.252, \quad \text{seu} \quad (x - g)(y - h) = 540.$$

Hinc autem reperiuntur sequentes numeri amicabiles:

$$\begin{cases} 8.\ 383.\ 1907 \\ 8.\ 11.\ 23.\ 2543 \end{cases} \qquad \begin{cases} 8.\ 467.\ 1151 \\ 8.\ 11.\ 23.\ 1871 \end{cases} \qquad \begin{cases} 8.\ 647.\ 719 \\ 8.\ 11.\ 23.\ 1619. \end{cases}$$

Hujusmodi numeris compositis pro f ponendis multi insuper alii inveniuntur numeri amicabiles.

§ 88. **Scholion.** Ingens combinationum numerus, qui in hoc exemplo locum habet, ansam mihi praebuit solutionem in aliam formam redigendi commodiorem. Scilicet cum sit

$$e = bf - (b - c)gh, \quad PQ = bbgh + be(f - 1) = (ex - bg)(ey - bh),$$

ex formulis $x = \frac{P + bg}{e}$ et $y = \frac{Q + bh}{e}$ eliciuntur valores

$$p = \frac{hP + bgh}{e} - 1, \quad q = \frac{gQ + bgh}{e} - 1, \quad r = \frac{PQ + b(hP + gQ) + bbgh}{ee} - 1.$$

Sit ergo ob $gh = ff$, $e = bf - (b - c)ff$, $L = bbff + be(f - 1)$ et $MN = Lff$, erit

$$p = \frac{M + bff}{e} - 1, \quad q = \frac{N + bff}{e} - 1, \quad r = \frac{L + b(M + N) + bbff}{ee} - 1$$

et nunc quaestio eo reducitur, ut numerus Lff resolvatur in duos factores M et N, quorum uterque quantitate bff auctus, fiat divisibilis per e, et ut quoti hinc resultantes unitate minuti, sint numeri primi. Denique oportet ut sit $r + 1 = \frac{(p + 1)(q + 1)}{ff}$, et r numerus primus. Hunc ergo calculum in nonnullis casibus illustrabo.

§ 89. **Casus III.** Sit $a = 2^4 = 16$, erit $b = 16$, $c = 1$, atque

$$e = 16f - 15ff, \quad L = 256ff + 16e(f - 1) \quad \text{et} \quad MN = Lff.$$

Numeri igitur primi esse debent:

$$p = \frac{M + 16\int f}{e} - 1, \quad q = \frac{N + 16\int f}{e} - 1, \quad r = \frac{L + 256\int f + 16(M+N)}{ee} - 1,$$

quibus inventis erunt numeri amicabiles: $16pq$ et $16fr$.

§ 90. *Exempl.* 1. Sit $f = 17$, erit

$$\int f = 18, \; e = 2, \; L = 1024.5 \text{ et } MN = 1024.5.18 = 2^{11}.3^2.5, \quad \text{atque}$$

$$p = \frac{M + 288}{2} - 1, \quad q = \frac{N + 288}{2} - 1, \quad r = \frac{512.19 + 16(M+N)}{4} - 1,$$

seu sit $M = 2m$, $N = 2n$, ut sit $mn = 2^9.3^2.5$, erit

$$p = m + 143, \quad q = n + 143 \quad \text{et} \quad r = 8(m+n) + 2431,$$

qui tres numeri debent esse primi, ut numeri amicabiles sint $16pq$ et $16.17.r$. Hoc autem succedit duobus modis, primo si $m = 24$, $n = 960$, et secundo si $m = 96$ et $n = 240$, unde numeri amicabiles prodeunt:

$$\begin{cases} 16.\ 167.\ 1103 \\ 16.\ \ 17.\ 10303 \end{cases} \qquad \begin{cases} 16.\ 383.\ 239 \\ 16.\ 17.\ 5119. \end{cases}$$

§ 91. *Exempl.* 2. Sit $f = 19$, erit

$$\int f = 20, \; e = 4, \; L = 128.49, \text{ et } MN = 512.5.49 = 2^9.5.7^2.$$

Ergo

$$p = \frac{M + 320}{4} - 1, \quad q = \frac{N + 320}{4} - 1, \quad r = \frac{128.89 + 16(M+N)}{16} - 1,$$

seu sit $M = 4m$ et $N = 4n$, ut sit $mn = 32.5.49 = 2^5.5.7^2$, erit

$$p = m + 79, \quad q = n + 79 \quad \text{et} \quad r = 4(m+n) + 711.$$

Hinc si $m = 70$, $n = 112$, prodeunt numeri amicabiles:

$$\begin{cases} 16.\ 149.\ 191 \\ 16.\ 19.\ 1439. \end{cases}$$

§ 92. *Exempl.* 3. Sit $f = 23$, erit

$$\int f = 24, \quad e = 8, \quad L = 256.5.7 \text{ et } MN = 2048.3.5.7 = 2^{11}.3.5.7.$$

$$p = \frac{M + 16.24}{8} - 1, \quad q = \frac{N + 16.24}{8} - 1, \quad r = \frac{256.59 + 16(M+N)}{64} - 1,$$

seu sit $M = 8m$, $N = 8n$ et $mn = 2^5.3.5.7$, erit

$$p = m + 47, \quad q = n + 47 \quad \text{et} \quad r = 2(m+n) + 235.$$

Hinc tres casus oriuntur

$$\begin{cases} m = 56, \\ n = 60, \end{cases} \qquad \begin{cases} m = 42, \\ n = 80, \end{cases} \qquad \begin{cases} m = 6, \\ n = 560. \end{cases}$$

et numeri amicabiles sunt:

$$\begin{cases} 16.\ 103.\ 107 \\ 16.\ \ 23.\ 467 \end{cases} \qquad \begin{cases} 16.\ 89.\ 127 \\ 16.\ 23.\ 479 \end{cases} \qquad \begin{cases} 16.\ 53.\ 607 \\ 16.\ 23.\ 1367. \end{cases}$$

§ 93. *Exempl.* 4. Sit $f = 31$, erit $\int f = 32$, $e = 16$, $L = 512.31$ et $MN = 2^{14}.31$,

$$p = \frac{M + 16.32}{16} - 1, \quad q = \frac{N + 16.32}{16} - 1, \quad r = \frac{16(M + N) + 512.47}{256} - 1.$$

Sit ergo $M = 16m$, $N = 16n$ ut sit $mn = 2^6.31$, erit

$$p = m + 31, \quad q = n + 31, \quad r = m + n + 93.$$

Hinc autem nulli prodeunt numeri amicabiles.

§ 94. *Exempl.* 5. Sit $f = 47$, $\int f = 48$, erit $e = 32$ et $L = 1024.5.7$ et $MN = 2^{14}.3.5.7$, unde

$$p = \frac{M + 16.48}{32} - 1, \quad q = \frac{N + 16.48}{32} - 1, \quad r = \frac{16(M + N) + 1024.47}{1024} - 1,$$

Sit $M = 32m$ et $N = 32n$, ut sit $mn = 2^4.3.5.7$, erit

$$p = m + 23, \quad q = n + 23, \quad r = \tfrac{1}{2}(m + n) + 46.$$

Ergo $m + n$ debet esse numerus impariter par, ut $\frac{1}{2}(m + n)$ fiat impar, quod evenit si vel m vel n sit impariter par. Sit $m = 30$, $n = 56$, erunt numeri amicabiles

$$\begin{cases} 16.\ 53.\ 79 \\ 16.\ 47.\ 89. \end{cases}$$

§ 95. *Exempl.* 6. Sit $f = 17.137$, erit $\int f = 18.138 = 4.27.23 = 2484$, $e = 4$, $L = 256.2484 + 64.2328 = 512.3.7.73$ et $MN = 2048.81.7.23.73$,

$$p = \frac{M + 16.2484}{4} - 1, \quad q = \frac{N + 16.2484}{4} - 1, \quad r = \frac{512.2775 + 16(M + N)}{16} - 1.$$

Sit $M = 4m$, $N = 4n$, erit $mn = 128.81.7.23.73$ et

$$p = m + 9935, \quad q = n + 9935 \quad \text{et} \quad r = 4(m + n) + 88799.$$

Sed hic semper prodit valor ipsius r major quam 100000, ita ut difficile sit discernere, utrum sit primus nec ne.

§ 96. *Exempl.* 7. Sit $f = 17.151$, erit $\int f = 18.152 = 16.9.19 = 2736$, $e = 32$ et $L = 1024.1967 = 1024.7.281$, atque $MN = 2^{14}.9.7.19.281$. Sit $M = 32m$, $N = 32n$, erit $mn = 16.9.7.19.281$ et

$$p = m + 1367, \quad q = n + 1367, \quad r = \tfrac{1}{2}(m + n) + 2650.$$

Sit $m = 2\mu$, $n = 8\nu$, erit $\mu\nu = 9.7.19.281$ et

$$p = 2\mu + 1367, \quad q = 8\nu + 1367, \quad r = \mu + 4\nu + 2650.$$

Hinc primum patet neque μ neque ν esse posse numerum formae $3\alpha + 2$; tum μ non posse desinere in 9 nec ν in 1, quibus observatis sequentes tantum resolutiones locum habent:

	*		*		*	*	
$\mu =$	3.281	7.19	21.281	21	63.281	3	1
$\nu =$	21.19	9.281	57	57.281	19	399.281	1197.281

quorum ii, qui asteriscis sunt notati, excluduntur ideo, ne p, q, vel r fiat per 7 divisibile. Quarta resolutio dabit hos numeros amicabiles:

$$\begin{cases} 16.\ 1409.\ 129503 \\ 16.\ 17.\ 151.\ 66739, \end{cases}$$

si modo hic numerus 129503 est primus.

§ 97. *Exempl.* 8. Sit $f = 17.167$, erit $\int f = 18.168 = 16.27.7 = 3024$, $e = 64$, $L = 2048.1797 = 2048.3.599$ et $MN = 2^{15}.3^4.7.599$. Sit $M = 64m$, $N = 64n$, erit $mn = 2^3.3^4.7.599$ et

$$p = m + 755, \quad q = n + 755, \quad r = \frac{1}{4}(m+n) + \frac{2173}{2}$$

Sit $m = 2\mu$, $n = 4\nu$, erit $\mu\nu = 3^4.7.599$ et

$$p = 2\mu + 755, \quad q = 4\nu + 755, \quad r = \nu + \frac{\mu+1}{2} + 1086.$$

Ubi patet esse oportere $\mu = 4\alpha - 1$, ne r fiat numerus par: nec $\mu = 3\alpha + 2$, nec $\nu = 3\alpha + 1$. Hinc prodeunt numeri amicabiles

$$\begin{cases} 16.809.51071 \\ 16.17.167.13679. \end{cases}$$

§ 98. **Casus IV.** Sit vel $a = 3^4.5$, vel $a = 3^2.7.13$, ut sit $b = 9$, $c = 2$, erit $e = 9f - 7\int f$, $L = 81\int f + 9e(f-1)$ et $MN = L\int f$, erit

$$p = \frac{M + 9\int f}{e} - 1, \quad q = \frac{N + 9\int f}{e} - 1, \quad r = \frac{9(M+N) + L + 81\int f}{ee} - 1,$$

qui numeri p, q, r si fuerint primi, erunt numeri amicabiles apq, afr.

§ 99. *Exempl.* Sit $f = 7$, $\int f = 8$, erit $e = 7$, $L = 2.27.19$, $MN = 16.27.19$, erit

$$p = \frac{M+72}{7} - 1, \quad q = \frac{N+72}{7} - 1, \quad r = \frac{9(M+N) + 2.27.31}{49} - 1.$$

Unde posito $M = 54$, $N = 152$, oriuntur numeri amicabiles

$$\left.\begin{matrix} a.17.31 \\ a.7.71 \end{matrix}\right\} \text{ seu } \begin{cases} 3^4.5.17.31 \\ 3^4.5.7.71. \end{cases}$$

§ 100. **Problema 4.** Invenire numeros amicabiles hujus formae: *agpq* et *ahr*, ubi p, q, r sint numeri primi, at g et h sive primi sive compositi dati, una cum factore communi a.

Solutio. Ex factore communi a quaeratur in minimis terminis fractis $\frac{b}{c} = \frac{a}{2a - \int a}$; deinde sit $\frac{\int g}{\int h} = \frac{m}{n}$, et ex prima proprietate numerorum amicabilium erit

$$(p+1)(q+1)\int g = (r+1)\int h, \text{ seu } r + 1 = \frac{m}{n}(p+1)(q+1).$$

Altera vero proprietas praebet $(r+1)\int a.\int h = a(gpq + hr)$, vel ob $\frac{\int a}{a} = \frac{2b-c}{b}$, erit

$$(r+1)(2b-c)\int h = b(gpq + hr),$$

et pro r substituto valore

$$m(2b-c)(p+1)(q+1)\int h = b(ngpq + mh(p+1)(q+1) - nh).$$

Sit brevitatis gratia $p + 1 = x$, $q + 1 = y$, erit

$$m(2b-c)xy\int h = b(mhxy + ngxy - ngx - ngy + ng - nh), \quad \text{vel}$$

$$(mbh + nbg - 2mb\int h + mc\int h)xy - nbgx - nbgy = nb(h-g).$$

Ponatur brevitatis gratia $e = b(mh + ng) - (2b-c)m\int h$, eritque

$$eexy - nbgex - nbgey + nnbbgg = nnbbgg + nb(h-g)e \quad \text{seu}$$
$$(ex - nbg)(ey - nbg) = nnbbgg + nb(h-g)e.$$

Ponatur ergo $nnbbgg + nb(h-g)e = MN$ fietque

$$x = \frac{M + nbg}{e} \quad \text{et} \quad y = \frac{N + nbg}{e} \quad \text{seu}$$
$$p = \frac{M + nbg}{e} - 1, \quad q = \frac{N + nbg}{e} - 1, \quad r = \frac{m}{n}xy - 1.$$

Qui tres numeri p, q et r si fuerint primi, erunt numeri amicabiles $agpq$ et ahr, dummodo utriusque factores sint primi inter se.

§ 101. **Coroll.** Si sint g et h numeri primi, erit $\frac{m}{n} = \frac{g+1}{h+1}$; sit ergo $g = km - 1$ et $h = kn - 1$, erit $\int h = kn$, unde fiet

$$e = b(2kmn - m - n) - (2b - c)kmn = ckmn - b(m+n)$$
$$MN = nb(nb(km-1)^2 + k(n-m)e) = (ex - bn(km-1))(ey - bn(km-1))$$
$$\text{et} \quad p = x - 1, \quad q = y - 1 \quad \text{atque} \quad r = \frac{m}{n}xy - 1.$$

§ 102. **Casus I.** Sit $m = 1$, $n = 3$, ergo $g = k - 1$, $h = 3k - 1$, eritque $e = 3ck - 4b$ et $MN = 3b(3b(k-1)^2 + 2ke)$ ideoque

$$x = \frac{M + 3b(k-1)}{e}, \quad y = \frac{N + 3b(k-1)}{e}$$

ac denique $p = x - 1$, $q = y - 1$ et $r = \frac{1}{3}xy - 1$.

§ 103. *Exempl.* 1. Sit $a = 4$, $b = 4$, $c = 1$, erit $e = 3k - 16$ et

$$MN = 12(12(k-1)^2 + 2ke) \quad \text{et} \quad x = \frac{M + 12(k-1)}{e} \quad \text{et} \quad y = \frac{N + 12(k-1)}{e}.$$

Hic poni potest

I. $k = 6$, fietque $g = 5$, $h = 17$ et $e = 2$, sed hinc nihil efficitur.

II. $k = 8$, fietque $g = 7$, $h = 23$ et $e = 8$, $MN = 12(12.49 + 128)$ seu

$$MN = 16.3.179 = (8x - 84)(8y - 84) \text{ ideoque } 3.179 = (2x - 21)(2y - 21),$$

unde nihil pariter sequitur.

§ 104. *Exempl.* 2. Sit $a = 8$, $b = 8$, $c = 1$, erit $e = 3k - 32$,

$$MN = 24(24(k-1)^2 + 2ke) \quad \text{seu}$$
$$MN = 48(15kk - 56k + 12) = (ex - 24(k-1))(ey - 24(k-1)).$$

Verum ne hinc quoque quicquam concludere licet.

§ 105. **Casus II.** Sit $m = 3$, $n = 1$, erit $e = 3ck - 4b$ et $g = 3k - 1$, $h = k - 1$,

$$MN = b(b(3k-1)^2 - 2ke) = (ex - b(3k-1))(ey - b(3k-1)), \quad \text{atque}$$
$$p = x - 1, \quad q = y - 1 \quad \text{et} \quad r = 3xy - 1.$$

§ 106. *Exempl.* 1. Sit $a = 10$, $b = 5$, $c = 1$, erit $e = 3k - 20$ et

$$5(5(3k-1)^2 - 2ke) = (ex - 5(3k-1))(ey - 5(3k-1)).$$

Si hic ponatur $k=8$, fiet $5.29.89=(4x-115)(4y-115)$. Unde prodit $x=30$, $y=674$, $3xy=60660$, et numeri amicabiles erunt

$$\begin{cases}10.23.29.673\\ 10.7.60659.\end{cases}$$

§ 107. *Exempl.* 2. Sit $a=3^2.5$, $b=9$, $c=2$, erit $e=6k-36$ et

$$9(3k-1)^2-2ke=(\tfrac{1}{2}ex-3(3k-1))(\tfrac{1}{2}ey-3(3k-1)).$$

Jam fiat $k=8$, erit $e=12$ et $3.1523=(4x-69)(4y-69)$, hincque oritur $x=18$, $y=398$, $3xy=21492$, eruntque numeri primi $g=23$, $h=7$, $p=17$, $q=397$, $r=21491$, et numeri amicabiles

$$\begin{cases}3^2.5.23.17.397\\ 3^2.5.7.21491.\end{cases}$$

§ 108. **Scholion.** Ex his exemplis usus hujus problematis in inveniendis numeris amicabilibus satis luculenter perspicitur; sed ob ipsam nimiam fingendi libertatem non parum molestum est secundum praecepta hic tradita omnes casus percurrere. Cum igitur sufficiat hanc methodum tradidisse ejusque usum monstrasse, ei prolixius non immoror, sed ad ultimam methodum, cujus ope numeros amicabiles eruere liceat, qua quidem sum usus, exponendam progredior. Nititur ea autem singularibus proprietatibus, quibus numeri ratione summae divisorum gaudent, quas oblata occasione explicabo, ne plurium lemmatum praemissio taedium creet. Iis autem expositis non difficile erit plura alia problemata ad hoc genus pertinentia resolvere.

§ 109. **Problema 5.** Invenire numeros amicabiles hujus formae zap et zbq, ubi factores a et b sint dati, p et q numeri primi, et factor communis z investigari debeat.

Solutio. Sit $\int a:\int b=m:n$, et cum esse debeat

$$\int a(p+1)=\int b(q+1),\ \text{ erit }\ m(p+1)=n(q+1).$$

Ponatur $p+1=nx$ et $q+1=mx$, eruntque numeri amicabiles: $za(nx-1)$ et $zb(mx-1)$. Ubi quidem requiritur ut $mx-1$ et $nx-1$ sint numeri primi. Cum jam utriusque numeri eadem sit summa divisorum $=nx\int a\int z=mx\int b\int z$, oportet ut ea sit aequalis summae numerorum $z((na+mb)x-a-b)$. Unde obtinetur ista aequatio $\frac{z}{\int z}=\frac{nx\int a}{(na+mb)x-a-b}$. Quo jam ex hac aequatione valor ipsius z elici queat, fractio $\frac{nx\int a}{(na+mb)x-a-b}$ ad minimos terminos reducatur, quae sit $=\frac{r}{s}$, ita ut habeatur $\frac{z}{\int z}=\frac{r}{s}$; hincque sequentia sunt notanda: Primo esse z vel ipsi r aequale, vel ejus multiplo cuipiam puta kr. Priori casu, si $z=r$, erit $\int z=s$, ac propterea $s=\int r$. Posteriori casu, si $z=kr$, erit $\int z=ks=\int kr$. Verum quicquid sit k, erit $\frac{\int kr}{\int r}>k$, nam $\int kr$ continet omnes divisores ipsius r singulos per k multiplicatos, et insuper eos divisores ipsius r, qui non sunt per k divisibiles; eritque ergo $\int kr>k\int r$. Cum igitur sit $\int z>k\int r$, erit quoque $ks>k\int r$, seu $s>\int r$. Quare si in fractione $\frac{r}{s}$ fuerit $s=\int r$, erit $z=r$; sin autem sit $s>\int r$, erit z aequale multiplo cuipiam ipsius r. Unde patet si sit $s<\int r$, aequationem $\frac{z}{\int z}=\frac{r}{s}$ esse impossibilem, neque hoc casu numeros amicabiles inveniri posse. Deinde cum sit

$\frac{\int z}{z} = \frac{na+mb}{n\int a} - \frac{a-b}{nx\int a} = \frac{a}{\int a} + \frac{b}{\int b} - \frac{a-b}{nx\int a}$, ob $\frac{a}{\int a} < 1$ et $\frac{b}{\int b} < 1$, erit $\frac{\int z}{z} < 2 - \frac{a-b}{nx\int a}$, ideoque multo magis $\frac{z}{\int z} > \frac{1}{2}$, ita ut z sit semper numerus deficiens. Hincque patet aequationem $\frac{z}{\int z} = \frac{r}{s}$ semper ita fore comparatam, ut sit $\frac{r}{s} > \frac{1}{2}$ seu $s < 2r$. Unde si sit $\int r = s$, erit $\int r < 2r$, et si $s > \int r$, erit multo magis $\int r < 2r$. Utroque igitur casu r erit numerus deficiens. Quocirca si x tanquam numerus incognitus spectetur, proposita aequatione

$$\frac{z}{\int z} = \frac{nx\int a}{(na+mb)x-a-b},$$

valorem ipsius x ita determinari oportet, ut reducta fractione $\frac{nx\int a}{(na+mb)x-a-b}$ ad minimos terminos $\frac{r}{s}$, fiat r numerus deficiens, et ut sit vel $s = \int r$, vel $s > \int r$. Quibus conditionibus animadversis, tam r quam s in suos factores simplices primos resolvatur, ut prodeat hujusmodi aequatio

$$\frac{z}{\int z} = \frac{A^\alpha B^\beta C^\gamma}{E^\epsilon F^\zeta G^\eta},$$

tunc autem successive vel A^α, vel altior potestas ipsius A ponatur factor ipsius z, seu ponatur

$$z = P.A^{\alpha+\nu}, \quad \text{erit } \int z = \int A^{\alpha+\nu}\int P \quad \text{et} \quad \frac{z}{\int z} = \frac{PA^{\alpha+\nu}}{\int A^{\alpha+\nu}\int P}, \quad \text{ideoque}$$

$$\frac{P}{\int P} = \frac{B^\beta C^\gamma \int A^{\alpha+\nu}}{A^\nu E^\epsilon F^\zeta G^\eta}.$$

Similique modo ponatur ulterius $P = B^{\beta+\mu}Q$, et hoc pacto procedatur, donec tandem perveniatur ad aequationem hujus formae $\frac{Z}{\int Z} = \frac{u}{\int u}$, ex qua habeatur $Z = u$. Saepe quidem haec operatio successu optato caret, sed pro quovis casu oblato facilius erit operationem hanc per exempla docere, quam per praecepta.

§ 110. *Exempl.* 1. Sit $a = 3$, $b = 1$, erit $\int a = 4$, $\int b = 1$ et $m = 4$, $n = 1$, ac numeri amicabiles erunt: $3(x-1)z$ et $(4x-1)z$, si sint $x-1$ et $4x-1$ numeri primi et $\frac{z}{\int z} = \frac{4x}{7x-4}$. Hic autem primo patet, si 4 ex numeratore non tollatur, fore $7x - 4 < \int 4x$, ob $\int 4x = 7\int x$. Ergo necesse est ut sit $7x-4$ numerus par. Ponatur $x = 4p$, erit $\frac{z}{\int z} = \frac{4p}{7p-1}$. Nunc fiat $7p-1$ numerus par, ponendo $p = 2q+1$, erit $\frac{z}{\int z} = \frac{2(2q+1)}{7q+3}$ et $x = 8q+4$, atque $x-1 = 8q+3$, $4x-1 = 32q+15$. Unde q nequit esse multiplum ternarii, ne $x-1$ fiat per 3 divisibile. Erit ergo vel $q = 3r+1$, vel $q = 3r-1$; priori casu fit $2q+1 = 6r+3$, ac z deberet esse divisibile per 3, quod pariter fieri nequit, quia in altero numero quaesito $3(x-1)z$ jam inest factor 3. Sit igitur $q = 3r-1$, erit $\frac{z}{\int z} = \frac{2(6r-1)}{21r-4}$ atque $x = 24r-4$, $x-1 = 24r-5$ et $4x-1 = 96r-17$. Cum autem z factorem 3 habere nequeat, nisi binarius ex numeratore $2(6r-1)$ tollatur, z erit divisibile per 2, et posito $z = 2y$ fieret

$$\frac{2y}{3\int y} = \frac{2(6r-1)}{21r-4} \quad \text{et} \quad \frac{y}{\int y} = \frac{3(6r-1)}{21r-4},$$

ideoque evaderet y et propterea quoque z per 3 divisibile, quod fieri nequit. Hanc ob rem iste binarius ex numeratore tolli debet, ponendo $r = 2s$, ut sit $x-1 = 48s-5$, $4x-1 = 192s-17$, eritque $\frac{z}{\int z} = \frac{12s-1}{21s-2}$. Jam si s sit numerus impar, ob z numerum imparem, fiet quoque

$$\int z = k(21s-2)$$

numerus impar, ex quo sequitur numerum z fore quadratum: sin autem s sit numerus par, factor communis z non erit quadratus. Evolvantur ergo ii ipsius s valores, qui efficiunt $x-1=48s-5$ et $4x-1=192s-17$ numeros primos, et dispiciatur utrum aequationi $\frac{z}{\int z}=\frac{12s-1}{24s-2}$ satisfieri queat. Sit $s=7$, erit $x-1=331$, $4x-1=1327$ et $\frac{z}{\int z}=\frac{83}{145}$. Jam cum z debeat esse quadratum, ponatur $z=83^2A$, erit $\int z=367.19\int A$ et $\frac{A}{\int A}=\frac{367.19}{5.29.83}$. Nunc autem ipsius A factor statui nequit 19^2, ob $\int 19^2=3.127$; prodiret enim 3 factor ipsius A; altioribus vero potestatibus sumendis, mox devenitur ad numeros tam grandes, ut facile pateat opus succedere non posse.

Si $s=12$, erit $x-1=571$, $4x-1=2287$ et $\frac{z}{\int z}=\frac{11.13}{2.125}$, quae neque 11^2 neque 13 pro factoribus ipsius z assumendo resolvi potest. Neque vero etiam ex majoribus valoribus pro s mihi quicquam praestare licuit.

§ 111. *Exempl.* 2. Sit $a=5$, $b=1$, erit $\int a=6$, $\int b=1$, $m=6$, $n=1$, et numeri amicabiles erunt $5(x-1)z$ et $(6x-1)z$, habebiturque $\frac{z}{\int z}=\frac{6x}{11x-6}$. Quae aequatio ut sit possibilis, ex numeratore $6x$ vel binarium, vel ternarium tollere oportet, quia alioquin numerator maneret numerus redundans. Habebimus ergo duos casus evolvendos.

I. Tollatur ex numeratore ternarius ponendo $x=3p$, erit $\frac{z}{\int z}=\frac{6p}{11p-2}$, nunc vero ponatur $p=3q+1$, eritque $\frac{z}{\int z}=\frac{2(3q+1)}{11q+3}$, et ob $x=9q+3$, numeri primi esse debent $x-1=9q+2$ et $6x-1=54q+17$, ubi patet q esse debere numerum imparem. Sit ergo $q=2r-1$, erit $x-1=18r-7$, $6x-1=108r-37$ et $\frac{z}{\int z}=\frac{2(6r-2)}{22r-8}=\frac{2(3r-1)}{11r-4}$. Evolvantur jam casus, quibus $18r-7$ et $108r-37$ fiunt numeri primi, qui sunt

1) $r=1$, erit $x-1=11$, $6x-1=71$ et $\frac{z}{\int z}=\frac{2.2}{7}=\frac{4}{7}$. Cum igitur hic sit $7=\int 4$, erit $z=4$, et numeri amicabiles erunt $\left\{\begin{matrix}4.\ 5.\ 11\\ 4.\ 71\ ,\end{matrix}\right\}$ quos quidem jam invenimus.

2) $r=2$, erit $x-1=29$, $6x-1=179$ et $\frac{z}{\int z}=\frac{2.5}{2.9}=\frac{5}{9}$. At z factorem 5 habere nequit.

3) $r=5$. erit $x-1=83$, $6x-1=503$ et $\frac{z}{\int z}=\frac{4.7}{3.17}$, at hic $3.17<\int 4.7$.

4) $r=8$, erit $x-1=137$, $6x-1=827$ et $\frac{z}{\int z}=\frac{23}{2.3.7}$. Ponatur $z=23P$, erit $\int z=24\int P$ et $\frac{P}{\int P}=\frac{24}{23}\cdot\frac{z}{\int z}=\frac{4}{7}$, unde $P=4$ et $z=4.23$, quam operationem ita breviter repraesento:

$$\frac{z}{\int z}=\frac{23}{2.3.7}\left\{\frac{23}{24}\right\}\frac{4}{7}\left\{\frac{4}{7}\right\},$$

unde fit $z=4.23$, et numeri amicabiles erunt: $\left\{\begin{matrix}4.\ 23.\ 5.\ 137\\ 4.\ 23.\ 827.\end{matrix}\right.$

Reliqui valores, quousque quidem examinavi, nullos dant numeros amicabiles.

II. Tollatur ex numeratore binarius, ponendo $x = 2p$, erit $\frac{z}{\int z} = \frac{6p}{11p-3}$. Nunc sit $p = 2q + 1$, erit $\frac{z}{\int z} = \frac{3(2q+1)}{11q+4}$, et numeri primi esse debebunt (ob $x = 4q + 2$): $x - 1 = 4q + 1$, $6x - 1 = 24q + 11$, quare esse nequit $q = 3a - 1$. Deinde cum z non esse debeat divisibile per 5, neque $2q + 1$, neque $4q + 1$, neque $24q + 11$ per 5 debet esse divisibile, unde excluduntur casus $q = 5a + 2$, $q = 5a + 1$. Rejectis ergo his aliisque valoribus inutilibus ipsius q, qui pro $x - 1$ et $6x - 1$ non praebent numeros primos, calculus ita se habebit:

q	$x - 1$	$6x - 1$	$\frac{z}{\int z} = \frac{3(2q+1)}{11q+4}$
3	13	83	$\frac{3.7}{37}$ nihil dat.
4	17	107	$\frac{3.9}{48} = \frac{9}{16} \left\{\frac{9}{13}\right\} \frac{13}{16} \left\{\frac{13}{14}\right\} \frac{7}{8} \left\{\frac{7}{8}\right\}$; $z = 9.7.13$, vel $\frac{9}{16} \left\{\frac{27}{40}\right\} \frac{5}{6} \left\{\frac{5}{6}\right\}$ ergo $z = 27.5$. Hic autem valor, ob $a = 5$, est inutilis. Erunt ergo numeri amicabiles: $\begin{cases} 9.\ 7.\ 13.\ 5.\ 17 \\ 9.\ 7.\ 13.\ 107. \end{cases}$
9	37	227	$\frac{3.19}{103}$ nihil dat.
10	41	251	$\frac{3.21}{114} = \frac{3.7}{2.19} \left\{\frac{7^2}{3.19}\right\} \frac{3^2}{2.7} \left\{\frac{3^2}{13}\right\} \frac{13}{14} \left\{\frac{13}{14}\right\}$; ergo $z = 3^2.\ 7^2.\ 13$, et numeri amicabiles erunt: $\begin{cases} 3^2.\ 7^2.\ 13.\ 5.\ 41 \\ 3^2.\ 7^2.\ 13.\ 251. \end{cases}$
18	73	443	$\frac{3.37}{202} = \frac{3.37}{2.101}$ nihil dat.
24	97	587	$\frac{3.49}{268} = \frac{3.49}{4.67}$ nihil dat.
28	113	683	$\frac{3.57}{312} = \frac{9.19}{8.39} = \frac{3.19}{8.13}$ nihil dat.
34	137	827	$\frac{3.69}{378} = \frac{23}{2.21} = \frac{23}{2.3.7} \left\{\frac{23}{24}\right\} \frac{4}{7} \left\{\frac{4}{7}\right\}$; $z = 4.23$, ut ante.
39	157	947	$\frac{3.79}{433}$ nihil dat.
45	181	1091	$\frac{3.91}{499} = \frac{3.7.13}{499}$ ut ante.
48	193	1163	$\frac{3.97}{532} = \frac{3.97}{4.7.19} = \frac{3.97}{4.133} \left\{\frac{97}{2.7^2}\right\} \frac{3.7}{2.19} \left\{\frac{7^2}{3.19}\right\} \frac{3^2}{2.7} \left\{\frac{3^2}{13}\right\} \frac{13}{14}$. Ergo $z = 3^2.\ 7^2.\ 13.\ 97$, et numeri amicabiles sunt: $\begin{cases} 3^2.\ 7^2.\ 13.\ 97.\ 5.\ 193 \\ 3^2.\ 7^2.\ 13.\ 97.\ 1163. \end{cases}$
49	197	1187	$\frac{3.99}{543} = \frac{9.11}{181}$
60	241	1451	$\frac{3.121}{664} = \frac{3.11^2}{8.83}$

q	$x-1$	$6x-1$	$\frac{z}{\int z}=\frac{3(2q+1)}{11q+4}$
69	277	1667	$\frac{3.139}{793}$
79	317	1907	$\frac{3.159}{873}=\frac{53}{97}$
84	337	2027	$\frac{3.169}{928}=\frac{3.169}{8.116}=\frac{3.169}{32.29}$
93	373	2243	$\frac{3.187}{1027}=\frac{3.11.17}{13.79}$
100	401	2411	$\frac{3.201}{1104}=\frac{3.67}{368}=\frac{3.67}{16.23}$
244	977	5867	$\frac{3.489}{2688}=\frac{3.163}{128.7}\left\{\frac{163}{4.41}\right\}\ \frac{3.41}{32.7}\left\{\frac{41}{2.3.7}\right\}\ \frac{3^2}{16}\left\{\frac{3^2}{13}\right\}\ \frac{13}{16}\left\{\frac{13}{14}\right\}\ \frac{7}{8}.$
			Ergo $z=3^2.7.13.41.163$, et numeri amicabiles erunt:
			$\begin{cases}3^2.\ 7.\ 13.\ 41.\ 163.\ 5.\ 977\\ 3^2.\ 7.\ 13.\ 41.\ 163.\ 5876.\end{cases}$

Hinc ergo bini prodierunt novi numeri amicabiles.

§ 112. *Exempl.* 3. Sit $a=7$, $b=1$, erit $\int a=8$, $\int b=1$, $m=8$, $n=1$, et numeri amicabiles: $7(x-1)z$ et $(8x-1)z$, existente $\frac{z}{\int z}=\frac{8x}{15x-8}$. Ac primo quidem x debet esse numerus par: ponatur ergo $x=2p$, erit $x-1=2p-1$, $8x-1=16p-1$ et $\frac{z}{\int z}=\frac{8p}{15p-4}$, quae aequatio est impossibilis, nisi potestas binarii in numeratore deprimatur, quia $15p-4\not<8p$. Ergo fiat $p=4q$, ut sit $x=8q$, $x-1=8q-1$, $8x-1=64q-1$ et $\frac{z}{\int z}=\frac{8q}{15q-1}$. Nunc sit $q=2r+1$, erit $\frac{z}{\int z}=\frac{4(2r+1)}{15r+7}$ et $x-1=16r+7$, $8x-1=128r+63$, quorum numerorum ut neuter sit per 3 divisibilis, neque erit $r=3u-1$, neque $r=3u$. Sit ergo $r=3s+1$, erit $\frac{z}{\int z}=\frac{4(6s+3)}{45s+22}$ seu $\frac{z}{\int z}=\frac{4.3(2s+1)}{45s+22}$ et $x-1=48s+23$, $8x-1=384s+191$.

Nunc vel ternarius vel quaternarius ex numeratore tolli debet. At ternarius tolli nequit, quia denominator nunquam per 3 est divisibilis; tollatur ergo quaternarius, ad quod pono $s=2t$, eritque $\frac{z}{\int z}=\frac{2.3(4t+1)}{45t+11}$. Nunc sit $t=2u-1$, erit $\frac{z}{\int z}=\frac{3(8u-3)}{45u-17}$: at est $s=4u-2$, ideoque numeri primi esse debent $x-1=192u-73$, $8x-1=1536u-577$.

u	$x-1$	$8x-1$	$\frac{z}{\int z}$
5	887	7103	$\frac{3.37}{208}=\frac{3.37}{16.13}\left\{\frac{37}{2.19}\right\}\ \frac{3.19}{8.13}\left\{\frac{19}{4.5}\right\}\ \frac{3.5}{2.13}\left\{\frac{5}{2.3}\right\}\ \frac{3^2}{13}.$ Ergo
			$z=3^2.5.19.37$, et numeri amicabiles erunt:
			$\begin{cases}3^2.\ 5.\ 19.\ 37.\ 7.\ 887\\ 3^2.\ 5.\ 19.\ 37.\ 7103.\end{cases}$

u	$x-1$	$8x-1$	$\frac{z}{\int z}$
11	2039	16319	$\frac{3.5.17}{4.107}$
13	2423	19391	$\frac{3.101}{8.71}$
26	4919	39359	$\frac{3.205}{1153}$

§ 113. *Exempl.* 4. Sit $a = 11$, $b = 1$, erit $\int a = m = 12$, $\int b = n = 1$; numeri quaesiti $11(x-1)z$ et $(12x-1)z$, atque $\frac{z}{\int z} = \frac{12x}{23x-12}$. Hic ex numeratore vel 3, vel 4 tolli debet.

I. Tollatur 3: ponatur $x = 3p$, erit $\frac{z}{\int z} = \frac{12p}{23p-4}$; et $p = 3q-1$, erit $\frac{z}{\int z} = \frac{4(3q-1)}{23q-9}$, et ob $x = 9q-3$, q debet esse impar. Sit $q = 2r+1$, ut sit $x = 18r+6$, erit

$$\frac{z}{\int z} = \frac{4(6r+2)}{46r+14} = \frac{4(3r+1)}{23r+7}$$

et $x-1 = 18r+5$, $12x-1 = 216r+71$.

r	$x-1$	$12x-1$	$\frac{z}{\int z}$
0	5	71	$\frac{4}{7}$, $z = 4$; numeri amicabiles $\begin{cases} 4.\ 11.\ 5 \\ 4.\ 71 \end{cases}$
2	41	503	$\frac{4.7}{53}$
3	59	719	$\frac{4.10}{76} = \frac{2.5}{19}$ imp.
6	113	1367	$\frac{4.19}{145} = \frac{4.19}{5.29}$ imp.
7	131	1583	$\frac{4.22}{168} = \frac{11}{21} = \frac{11}{3.7}$ $\left\{\frac{11}{12}\right\}$ $\frac{4}{7}$, sed ob factorem 11 hic valor z non valet.

II. Tollatur factor 4, ac ponatur $x = 4p$, ut fiat $\frac{z}{\int z} = \frac{12p}{23p-3}$. Jam sit $p = 4q+1$, erit $\frac{z}{\int z} = \frac{3(4q+1)}{23q+5}$, et ob $x = 16q+4$ numeri primi esse debent

$$x-1 = 16q+3 \quad \text{et} \quad 12x-1 = 192q+47;$$

hinc excluduntur valores $q = 3\alpha$.

q	$x-1$	$12x-1$	$\frac{z}{\int z}$
0	3	47	$\frac{3}{5}$ imposs.
1	19	239	$\frac{3.5}{4.7}$ $\left\{\frac{5}{2.3}\right\}$ $\frac{3^2}{14}$ $\left\{\frac{3^2}{13}\right\}$ $\frac{13}{14}$; $z = 3^2.5.13$, et numeri amicabiles erunt: $\begin{cases} 3^2.\ 5.\ 13.\ 11.\ 19 \\ 3^2.\ 5.\ 13.\ 239. \end{cases}$

q	$x-1$	$12x-1$	$\frac{z}{\int z}$
13	211	2543	$\frac{3.53}{16.19}$ $\left\{\frac{53}{2.27}\right\}$ $\frac{81}{8.19}$ $\left\{\frac{243}{4.7.13}\right\}$ $\frac{7.13}{2.3.19}$ $\left\{\frac{13}{2.7}\right\}$ $\frac{7^2}{3.19}$ $\left\{\frac{7^2}{3.19}\right\}$
			Ergo $z=3^5.7^2.13.53$, et numeri amicabiles erunt: $\begin{cases}3^5.7^2.13.53.11.211\\3^5.7^2.13.53.2543.\end{cases}$

§ 114. *Exempl.* 5. Sit $a=5$, $b=17$ et numeri amicabiles $5(3x-1)z$ et $17(x-1)z$, erit $\frac{z}{\int z}=\frac{18x}{32x-22}=\frac{9x}{16x-11}$. Cum x debeat esse numerus par, ponatur $x=2p$, erit $\frac{z}{\int z}=\frac{18p}{32p-11}$, et ex numeratore $18p$ vel factor 2 vel 3^2 tolli debet, ne sit numerus redundans. At factor 2 tolli nequit; tollatur ergo factor 9. Ad hoc ponatur $p=9q+4$, ut sit $x=18q+8$ et $x-1=18q+7$ et $3x-1=54q+23$, erit $\frac{z}{\int z}=\frac{2(9q+4)}{32q+13}$.

q	$x-1$	$12x-1$	$\frac{z}{\int z}$
0	7	23	$\frac{8}{13}$ imposs.
2	43	131	$\frac{4.11}{7.11}=\frac{4}{7}$, $z=4$, et numeri amicabiles: $\begin{cases}4.5.131\\4.17.43\end{cases}$
4	79	239	$\frac{16.5}{3.47}$
5	97	293	$\frac{2.49}{173}$
17	313	941	$\frac{2.157}{557}$
19	349	1049	$\frac{2.5^2.7}{27.23}$
20	367	1103	$\frac{16.23}{653}$
24	439	1319	$\frac{8.5.11}{781}$ inut. $=\frac{8.5}{71}$.

§ 115. *Exempl.* 6. Sit $a=37$ et $b=227$, erit $\int a=38$, $\int b=228$ et $\frac{m}{n}=\frac{1}{6}$; unde si numeri amicabiles sint $37(6x-1)z$ et $227(x-1)z$, fiet $\frac{z}{\int z}=\frac{6.38x}{449x-264}=\frac{4.3.19x}{449x-264}$, ubi cum x debeat esse numerus par, ponatur $x=2p$, ut numeri primi esse debeant $x-1=2p-1$ et $6x-1=12p-1$, eritque $\frac{z}{\int z}=\frac{4.3.19p}{44p-132}$. Nunc ex numeratore vel factor 4, vel factor 3 tolli debet.

I. Tollatur factor 3; ad hoc ponatur $p=3q$, ut sit $\frac{z}{\int z}=\frac{4.3.19q}{449q-44}$; nunc fiat $q=3r+1$, eritque $\frac{z}{\int z}=\frac{4.19(3r+1)}{449r+135}$ et $p=9r+3$, $x-1=18r+5$, $6x-1=108r+35$.

r	$x-1$	$6x-1$	$\frac{z}{\int z}$
2	41	251	$\frac{4.19.7}{1033}$
3	59	359	$\frac{4.19.10}{1482} = \frac{4.5}{3.13}$
6	113	683	$\frac{4.19.19}{3.23.41}$
13	239	1439	$\frac{4.19.40}{4.1493}$
17	311	1871	$\frac{16.13.19}{8.971}$
22	401	2411	$\frac{4.19.67}{10013} = \frac{4.67}{17.31} \left\{\frac{67}{4.17}\right\} \frac{16}{31} \left\{\frac{16}{31}\right\}$; $z = 16.67$
			numeri amicabiles: $\begin{cases} 16.\ 67.\ 37.\ 2411 \\ 16.\ 67.\ 227.\ 401. \end{cases}$
117	2111	12671	$\frac{4.19.352}{52668} = \frac{128.11.19}{4.7.9.11.19} = \frac{32}{63}$; $z = 32$,
			et numeri amicabiles: $\begin{cases} 32.\ 37.\ 12671 \\ 32.\ 227.\ 2111. \end{cases}$

II. Tollatur factor 4; ponatur $p = 4q$, erit $\frac{z}{\int z} = \frac{4.3.19q}{449q - 33}$; nunc sit $q = 4r + 1$, erit $p = 16r + 4$, $x - 1 = 32r + 7$, $6x - 1 = 192r + 47$ atque $\frac{z}{\int z} = \frac{3.19(4r+1)}{449r + 104}$.

r	$x-1$	$6x-1$	$\frac{z}{\int z}$
0	7	47	$\frac{3.19}{8.13} \left\{\frac{19}{4.5}\right\} \frac{3.5}{2.13} \left\{\frac{5}{2.3}\right\} \frac{3^2}{13}$; $z = 3^2.5.19$ et numeri amicabiles:
			$\begin{cases} 3^2.\ 5.\ 19.\ 37.\ 47 \\ 3^2.\ 5.\ 19.\ 227.\ 7. \end{cases}$
2	71	431	$\frac{9.19}{2.167}$
8	263	1583	$\frac{3.19.33}{16.3.7.11} = \frac{3.19}{16.7} \left\{\frac{19}{4.5}\right\} \frac{3.5}{4.7} \left\{\frac{5}{2.3}\right\} \frac{3^2}{2.7} \left\{\frac{3^2}{13}\right\} \frac{13}{14}$; $z = 3^2.5.13.19$,
			et numeri amicabiles: $\begin{cases} 3^2.\ 5.\ 13.\ 19.\ 37.\ 1583 \\ 3^2.\ 5.\ 13.\ 19.\ 227.\ 263, \end{cases}$
15	487	2927	$\frac{3.19.61}{7.977}$
23	743	4463	$\frac{9.19.31}{9.19.61} = \frac{31}{61}$
26	839	5039	$\frac{3.19.105}{2.3.13.151} = \frac{3.5.7.19}{2.13.151}$
30	967	5807	$\frac{3.19.11}{2.617}$
41	1319	7919	$\frac{3.19.165}{9.121.17} = \frac{5.19}{11.17}$.

§ 116. *Exempl.* 7. Sit $a = 79$, $b = 11.19 = 209$, $\int a = 80$, $\int b = 240$, erit $m = 1$, $n = 3$, et numeri amicabiles sint $79(3x-1)z$ et $11.19(x-1)z$, erit

$$\frac{z}{\int z} = \frac{240x}{446x - 288} = \frac{120x}{223x - 144}.$$

Sit $x = 2p$, erit $\frac{z}{\int z} = \frac{120p}{223p - 72}$ et numeri primi esse debent $2p - 1$ et $6p - 1$. Nunc autem ex numeratore $120p$ vel factor 8 vel 3 tolli debet.

I. Tollatur factor 3; sit $p = 9q$, erit $\frac{z}{\int z} = \frac{120q}{223q - 8}$, et fiat $q = 3r - 1$, ut sit $\frac{z}{\int z} = \frac{40(3r-1)}{223r - 77}$, $p = 27r - 9$ et $x - 1 = 54r - 19$, ac $3x - 1 = 162r - 55$. Nunc autem ob 40 numerum redundantem vel 5 vel 4 tolli debet:

α) Tollatur 5, sitque $r = 5s - 1$, erit $\frac{z}{\int z} = \frac{8(15s-4)}{223s - 60}$, et numeros primos esse oportet $x - 1 = 470s - 73$, $3x - 1 = 810s - 217$. Ac ne ternarius denuo in numeratorem intret, excludendi sunt casus $s = 3u - 1$. Hinc autem nihil invenitur.

β) Cum sit $\frac{z}{\int z} = \frac{40(3r-1)}{223r - 77}$, tollatur 4: sitque $r = 4s - 1$, erit $\frac{z}{\int z} = \frac{10(12s-4)}{223s - 75} = \frac{40(3s-1)}{223s - 75}$; Sit porro $s = 4t + 1$, erit $\frac{z}{\int z} = \frac{10(12t+2)}{223t + 37} = \frac{20(6t+1)}{223t + 37}$. Sit porro $t = 2u - 1$, erit $\frac{z}{\int z} = \frac{10(12u-5)}{223u - 93}$, et ob $r = 16t + 3 = 32u - 13$, erit $x - 1 = 1728u - 721$, et $3x - 1 = 5184u - 2161$. At hos numeros non reddit primos valor minor ipsius u quam 16, unde fit $\frac{z}{\int z} = \frac{2.11.17}{5.139}$, qui ob factorem 11 est inutilis.

II. Ergo ex aequatione $\frac{z}{\int z} = \frac{120p}{223p - 72}$ tollatur factor 8. Ponatur $p = 8q$, erit $\frac{z}{\int z} = \frac{120q}{223q - 9}$ et nunc sit $q = 8r - 1$, erit $\frac{z}{\int z} = \frac{3.5(8r-1)}{223r - 29}$; at ob $p = 64r - 8$, erit $x - 1 = 128r - 17$, $3x - 1 = 384r - 49$, unde valores excluduntur $r = 3a + 1$ et $r = 5a \pm 1$.

r	$x-1$	$3x-1$	$\frac{z}{\int z}$
2	239	719	$\frac{3.5^2}{139}$
3	367	1103	$\frac{3.23}{128}\left\{\frac{23}{8.3}\right\}\frac{3^2}{16}\left\{\frac{3^2}{13}\right\}\frac{13}{16}\left\{\frac{13}{14}\right\}\frac{7}{8}$. Ergo $z = 3^2.7.13.23$, vel
			$\frac{3.23}{128}\left\{\frac{23}{8.3}\right\}\frac{3^2}{16}\left\{\frac{3^3}{8.5}\right\}\frac{5}{6}$, ergo $z = 3^3.5.23$, et numeri amicabiles
			erunt: $\begin{cases} 3^2.\,7.\,13.\,23.\,79.\,1103 \\ 3^2.\,7.\,13.\,23.\,11.\,19.\,367 \end{cases}$
			vel $\begin{cases} 3^3.\,5.\,23.\,79.\,1103 \\ 3^3.\,5.\,23.\,11.\,19.\,367. \end{cases}$

§ 117. *Exempl.* 8. Sit $a = 17.19$, $b = 11.59$, erit $\int a = 18.20$, $\int b = 12.60$, et $m = 1$, $n = 2$. Si ergo numeri amicabiles ponantur $17.19(2x-1)z$ et $11.59(x-1)z$, erit

$$\frac{z}{\int z} = \frac{720x}{1295x - 972}.$$

Sit $x = 2p$, erit $\frac{z}{\int z} = \frac{720p}{1295p - 486}$, atque $x - 1 = 2p - 1$, $2x - 1 = 4p - 1$, quorum ut neuter sit divisibilis per 3, debet esse $p = 3q$, ut sit $\frac{z}{\int z} = \frac{720q}{1295q - 162}$ et $x - 1 = 6q - 1$, $2x - 1 = 12q - 1$. Tollatur ex numeratore factor 16, sitque $q = 2r$, erit $\frac{z}{\int z} = \frac{720r}{1295r - 81}$; nunc sit $r = 16s - 1$, erit $\frac{z}{\int z} = \frac{45(16s - 1)}{1295s - 86}$ et $x - 1 = 192s - 13$, $2x - 1 = 384s - 25$. Sit $s = 1$, erit $x - 1 = 179$, $2x - 1 = 359$ et

$$\frac{z}{\int z} = \frac{45.15}{1209} = \frac{225}{403} = \frac{3^2.5^2}{13.31} \left\{\frac{3^2}{13}\right\} \frac{5^2}{31} \left\{\frac{5^2}{31}\right\}.$$

Ergo $z = 3^2.5^2$, et numeri amicabiles erunt: $\begin{cases} 3^2.\ 5^2.\ 17.\ 19.\ 359 \\ 3^2.\ 5^2.\ 11.\ 59.\ 179. \end{cases}$

§ 118. **Scholion.** Haec ultima methodus in problemate 5 exposita prorsus diversa est a methodo praecedente, quam problemata quatuor priora complectuntur: dum in hac factor communis quaeritur, in illa autem datur. Utraque tamen singulari praestantiae genere est praedita, ut altera sine subsidio alterius non satis apta sit ad multitudinem numerorum amicabilium augendam. Posterior enim methodus suppeditat ejusmodi factores communes, quos ad usum prioris vix suspicari licuisset: prior vero suggerit reliquos factores huic instituto idoneos. Ceterum cuncta, quae hic tradidi, specimen continent methodi summe incertae, quam, quantum licuit, ad regulas algebraicas reduxi, ut vaga tentandi incertitudo restringeretur. Coronidis ergo loco ultra sexaginta numerorum amicabilium paria subjungam, quos his methodis elicui.

Catalogus numerorum amicabilium.

I.	$2^2.5.11$ $2^2.71$	X.	$3^2.5.19.37.7.887$ $3^2.5.19.37.7103$	XIX.	$2^4.23.479$ $2^4.89.127$
II.	$2^4.23.47$ $2^4.1151$	XI.	$3^4.5.11.29.89$ $3^4.5.11.2699$	XX.	$2^4.23.467$ $2^4.103.107$
III.	$2^7.191.383$ $2^7.73727$	XII.	$3^2.7^2.11.13.41.461$ $3^2.7^2.11.13.19403$	XXI.	$2^4.17.5119$ $2^4.239.383$
IV.	$2^2.23.5.137$ $2^2.23.827$	XIII.	$3^2.5.13.19.29.569$ $3^2.5.13.19.17099$	XXII.	$2^4.17.10303$ $2^4.167.1103$
V.	$3^2.7.13.5.17$ $3^2.7.13.107$	XIV.	$3^2.7^2.13.97.5.193$ $3^2.7^2.13.97.1163$	XXIII.	$2^4.19.1439$ $2^4.149.191$
VI.	$3^2.5.13.11.19$ $3^2.5.13.239$	XV.	$3^2.7.13.41.163.5.977$ $3^2.7.13.41.163.5867$	XXIV.	$2^5.59.1103$ $2^5.79.827$
VII.	$3^2.7^2.13.5.41$ $3^2.7^2.13.251$	XVI.	$2^3.17.79$ $2^3.23.59$	XXV.	$2^5.37.12671$ $2^5.227.2111$
VIII.	$3^2.5.7.53.1889$ $3^2.5.7.102059$	XVII.	$2^4.23.1367$ $2^4.53.607$	XXVI.	$2^5.53.10559$ $2^5.79.7127$
IX.	$2^2.13.17.389.509$ $2^2.13.17.198899$	XVIII.	$2^4.47.89$ $2^4.53.79$	XXVII	$2^6.79.11087$ $2^6.383.2309$

XXVIII.	$2^8. 383. 9203$ $2^8. 1151. 3067$	XXXIX.	$2. 5. 7. 19. 107$ $2. 5. 47. 359$	L.	$2^4. 23. 47. 9767$ $2^4. 1583. 7103$
XXIX.	$2^2. 11. 17. 263$ $2^2. 11. 43. 107$	XL.	$2^3\ 11. 163. 191$ $2^3. 31. 11807$	LI.	$2^2. 5. 13. 1187$ $2^2. 43. 2267$
XXX.	$3^2. 5. 7. 71$ $3^2. 5. 17. 31$	XLI.	$3^2. 7. 13. 23. 11. 19. 367$ $3^2. 7. 13. 23. 79. 1103$	LII.	$3^2. 7. 13. 5. 17. 1187$ $3^2. 7. 13. 131. 971$
XXXI.	$3^2. 5. 13. 29. 79$ $3^2. 5. 13. 11. 199$	XLII.	$3^3. 5. 23. 11. 19. 367$ $3^3. 5. 23. 79. 1103$	LIII.	$3^5. 7^2. 13. 53. 11. 211$ $3^5. 7^2. 13. 53. 2543$
XXXII.	$3^2. 5. 13. 19. 47$ $3^2. 5. 13. 29. 31$	XLIII.	$2^3. 11. 59. 173$ $2^3. 57. 2609$	LIV.	$3^2. 5^2. 11. 59. 179$ $3^2. 5^2. 17. 19. 359$
XXXIII.	$3^2. 5. 13. 19. 37. 1583$ $3^2. 5. 13. 19. 227. 263$	XLIV.	$2^3. 11. 23. 2543$ $2^3. 383. 1907$	LV.	$3^2\ 5. 17. 23\ 397$ $3^2. 5. 7. 21491$
XXXIV.	$3^2. 7^2. 13. 19. 11. 220499$ $3^2. 7^2. 13. 19. 89. 29399$	XLV.	$2^3. 11. 23. 1871$ $2^3. 467. 1151$	LVI.	$3^4. 7. 11^2. 19. 47. 7019$ $3^4. 7. 11^2. 19. 389. 863$
XXXV.	$3^2. 5. 19. 37. 47$ $3^2. 5. 19. 7. 227$	XLVI.	$2^3. 11. 23. 1619$ $2^3. 719. 647$	LVII.	$3^4. 7. 11^2. 19. 53. 6959$ $3^4. 7. 11^2. 19. 179. 2087$
XXXVI.	$2^4. 67. 37. 2411$ $2^4. 67. 227. 401$	XLVII.	$2^3. 11. 29. 239$ $2^3. 191. 449$	LVIII.	$3^5. 7^2. 13. 19. 47. 7019$ $3^5\ 7^2. 13. 19. 389. 863$
XXXVII	$3^3. 5. 7. 11. 29$ $3^3. 5. 31. 89$	XLVIII.	$2^3. 29. 47. 59$ $2^3. 17. 4799$	LIX.	$3^5. 7^2. 13. 19. 53. 6959$ $3^5. 7^2. 13\ 19. 179. 2087.$
XXXVIII.	$2. 5. 23. 29. 673$ $2. 5. 7. 60659$	XLIX.	$2^4. 17. 167. 13679$ $2^4. 809. 51071$		

His adjicere lubet duo paria sequentia, quae sunt formae diversae a praecedentibus:

LX.	$2^3. 19. 41$ $2^5. 199$	LXI.	$2^3. 41. 467$ $2^5. 19. 233.$

XI.

Observatio de summis divisorum.

(N. Comment. V. 1754—55. p. 59. Exhib. 1752. Apr. 6.)

§ 1. Proposito quocunque numero n, denotet haec formula $\int n$ summam omnium divisorum numeri n. Ita cum unitas praeter se ipsam alium non habeat divisorem, erit $\int 1 = 1$; atque cum numerus primus duos tantum habeat divisores, unitatem et se ipsum, si n fuerit numerus primus, erit $\int n = 1 + n$. Deinde cum numerus perfectus aequalis sit summae suarum partium aliquotarum, partes aliquotae autem sint divisores ejus praeter ipsum numerum, manifestum est numeri perfecti summam divisorum se ipso esse duplo majorem, hinc si n sit numerus perfectus, erit $\int n = 2n$. Porro quoniam numerus redundans appellari solet is, cujus summa partium aliquotarum ipso est major, si n sit numerus redundans, erit $\int n > 2n$; ac si n sit numerus deficiens, seu talis, cujus summa partium aliquotarum ipso est minor, erit $\int n < 2n$.

§ 2. Hoc igitur modo indoles numerorum, quatenus summa partium aliquotarum, vel divisorum, continetur, facile signis exprimitur. Si enim fuerit $\int n = 1 + n$, erit n numerus primus, si sit $\int n = 2n$, erit n numerus perfectus, ac si sit vel $\int n > 2n$, vel $\int n < 2n$, numerus n erit vel redundans, vel deficiens. Huc etiam referri potest quaestio de numeris, qui amicabiles vocari solent, quorum alter summae partium aliquotarum alterius aequatur. Si enim sint m et n numeri amicabiles, cum numeri m sit summa partium aliquotarum $= \int m - m$, et numeri $n = \int n - n$, erit ex natura horum numerorum $n = \int m - m$ et $m = \int n - n$, sicque habebitur $\int m = \int n = m + n$. Duo ergo numeri amicabiles eandem divisorum summam habent, quae simul summae amborum numerorum est aequalis.

§ 3. Quo summa divisorum cujusque numeri propositi facilius inveniri possit, id commodissime fiet hunc numerum in duos factores, qui inter se sint primi, resolvendo. Si enim sint p et q numeri inter se primi, seu qui praeter unitatem nullum habeant divisorem communem, tum summa divisorum producti pq aequalis erit producto ex summis divisorum utriusque, seu erit $\int pq = \int p . \int q$. Hinc inventis summis divisorum numerorum minorum, inventio summae divisorum non difficulter ad numeros majores extenditur.

§ 4. Si sint a, b, c, d, etc. numeri primi, omnis numerus, quantuscunque fuerit, semper ad hujusmodi formam $a^\alpha\, b^\beta\, c^\gamma\, d^\delta$ etc. reducitur: qua forma inventa, erit hujus numeri summa divisorum seu $\int a^\alpha b^\beta c^\gamma d^\delta$ etc. $= \int a^\alpha . \int b^\beta . \int c^\gamma . \int d^\delta$. etc. At ob a, b, c, d, etc. numeros primos, erit

$$\int a^\alpha = 1 + a + a^2 + \ldots\ldots + a^\alpha = \frac{a^{\alpha+1} - 1}{a - 1}, \quad \text{ideoque}$$

$$\int a^\alpha b^\beta c^\gamma d^\delta \text{ etc.} = \frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \cdot \frac{c^{\gamma+1} - 1}{c - 1} \cdot \frac{d^{\delta+1} - 1}{d - 1} \cdot \text{ etc.}$$

Sufficiet ergo singularum potestatum numerorum primorum tantum summas divisorum invenisse.

§ 5. Hanc autem indagationem ulterius non persequor, sed, ut ad id, quod hic tractare institui, propius accedam, numerorum secundum ordinem naturalem progredientium summas divisorum hic conspectui exponam.

∫ 1 = 1	∫26 = 42	∫51 = 72	∫ 76 = 140
∫ 2 = 3	∫27 = 40	∫52 = 98	∫ 77 = 96
∫ 3 = 4	∫28 = 56	∫53 = 54	∫ 78 = 168
∫ 4 = 7	∫29 = 30	∫54 = 120	∫ 79 = 80
∫ 5 = 6	∫30 = 72	∫55 = 72	∫ 80 = 186
∫ 6 = 12	∫31 = 32	∫56 = 120	∫ 81 = 121
∫ 7 = 8	∫32 = 63	∫57 = 80	∫ 82 = 126
∫ 8 = 15	∫33 = 48	∫58 = 90	∫ 83 = 84
∫ 9 = 13	∫34 = 54	∫59 = 60	∫ 84 = 224
∫10 = 18	∫35 = 48	∫60 = 168	∫ 85 = 108
∫11 = 12	∫36 = 91	∫61 = 62	∫ 86 = 132
∫12 = 28	∫37 = 38	∫62 = 96	∫ 87 = 120
∫13 = 14	∫38 = 60	∫63 = 104	∫ 88 = 180
∫14 = 24	∫39 = 56	∫64 = 127	∫ 89 = 90
∫15 = 24	∫40 = 90	∫65 = 84	∫ 90 = 234
∫16 = 31	∫41 = 42	∫66 = 144	∫ 91 = 112
∫17 = 18	∫42 = 96	∫67 = 68	∫ 92 = 168
∫18 = 39	∫43 = 44	∫68 = 126	∫ 93 = 128
∫19 = 20	∫44 = 84	∫69 = 96	∫ 94 = 144
∫20 = 42	∫45 = 78	∫70 = 144	∫ 95 = 120
∫21 = 32	∫46 = 72	∫71 = 72	∫ 96 = 252
∫22 = 36	∫47 = 48	∫72 = 195	∫ 97 = 98
∫23 = 24	∫48 = 124	∫73 = 74	∫ 98 = 171
∫24 = 60	∫49 = 57	∫74 = 114	∫ 99 = 156
∫25 = 31	∫50 = 93	∫75 = 124	∫100 = 217

§ 6. Si jam contemplemur seriem horum numerorum 1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28 etc. quam summae divisorum numeris naturali ordine procedentibus respondentes constituunt, non solum nulla lex progressionis patet, sed ordo horum numerorum tantopere est perturbatus, ut nulli prorsus legi adstrictus videatur. Quin etiam haec series ordinem numerorum primorum manifesto implicat, cum terminus indicis n seu $\int n$ toties sit $= n + 1$, quoties n est numerus primus; constat autem, numeros primos nullo adhuc modo ad certam quandam progressionis legem revocari potuisse. Cum autem nostra series non solum numerorum primorum, sed etiam omnium reliquorum numerorum, quatenus ex primis sunt compositi, rationem complectatur, ejus lex multo etiam difficilior inventu videtur, quam ipsius seriei numerorum primorum.

§ 7. Quae cum ita sint, non parum equidem mihi scientiam numerorum promovisse videor, dum certam atque constantem legem detexi, secundum quam termini seriei propositae 1, 3, 4, 7,

6, etc. progrediantur, ita ut per hanc legem quilibet istius seriei terminus ex praecedentibus definiri possit, inveni enim, quod magis mirum videatur, hanc seriem ad id genus progressionum pertinere, quae recurrentes vocari solent; et quarum natura ita est comparata, ut quilibet terminus ex praecedentibus secundum certam quandam relationis rationem determinetur. Quis autem unquam crediderit hanc seriem tantopere perturbatam, et quae cum seriebus recurrentibus nihil plane commune habere videtur, nihilominus in hoc serierum genere contineri ejusque scalam relationis assignari posse?

§ 8. Cum hujus seriei terminus indici n respondens, qui indicat summam divisorum numeri n, sit $= \int n$, ejus termini antecedentes ordine retrogrado erunt $\int(n-1)$, $\int(n-2)$, $\int(n-3)$, $\int(n-4)$, $\int(n-5)$ etc. Quilibet autem terminus istius seriei, scilicet $\int n$, ita ex aliquot antecedentium conflatur, ut sit:

$$\begin{aligned}\int n = & \int(n-1)+\int(n-2)-\int(n-5)-\int(n-7)+\int(n-12)+\int(n-15)-\int(n-22)\\ & -\int(n-26)+\int(n-35)+\int(n-40)-\int(n-51)-\int(n-57)+\int(n-70)+\int(n-77)\\ & -\int(n-92)-\int(n-100)+\int(n-117)+\int(n-126)-\text{etc.}\end{aligned}$$

Vel cum signa + et — alternatim binos terminos afficiant, haec series commode in duas divellitur, hoc modo:

$$\int n = \begin{cases}\int(n-1)-\int(n-5)+\int(n-12)-\int(n-22)+\int(n-35)-\int(n-51)+\text{etc.}\\ \int(n-2)-\int(n-7)+\int(n-15)-\int(n-26)+\int(n-40)-\int(n-57)+\text{etc.}\end{cases}$$

§ 9. Ex hac posteriori forma ordo numerorum, qui in utraque serie successive a numero n subtrahuntur, facile perspicitur, utraque enim series est secundi ordinis, differentias secundas habens constantes. Namque prioris seriei numeri cum suis differentiis tam primis, quam secundis, sunt:

	1,	5,	12,	22,	35,	51,	70,	92,	117,	etc.
diff. 1:	4,	7,	10,	13,	16,	19,	22,	25,	etc.	
diff. 2:	3,	3,	3,	3,	3,	3,	3,	etc.		

Unde illius seriei terminus generalis est $= \frac{3xx-x}{2}$, continetque adeo omnes numeros pentagonales. Altera series est:

	2,	7,	15,	26,	40,	57,	77,	100,	126,	etc.
diff. 1:	5,	8,	11,	14,	17,	20,	23,	26,	etc.	
diff. 2:	3,	3,	3,	3,	3,	3,	3,	etc.		

ideoque terminum generalem habet $\frac{3xx+x}{2}$, ac seriem numerorum pentagonalium retro continuatam continet.

§ 10. Omnino hic notatu est dignum, seriem numerorum pentagonalium tam ipsam, quam retro continuatam, ad ordinem seriei summarum divisorum potissimum adhiberi, cum sane nullum nexum inter numeros pentagonales et summas divisorum ne suspicari quidem liceat. Si enim series numerorum pentagonalium tam antrorsum, quam retrorsum continuata exponatur hoc modo:

etc. 77, 57, 40, 26, 15, 7, 2, 0, 1, 5, 12, 22, 35, 51, 70, 92, etc.

formula nostra ordinem summarum divisorum complectens signis alternantibus hoc modo ordinata exhiberi poterit:

$$\text{etc.} -\int(n-15)+\int(n-7)-\int(n-2)+\int(n-0)-\int(n-1)+\int(n-5)-\int(n-12)+\int(n-22)-\text{etc.}=0$$

quae series utrinque quidem in infinitum excurrit, sed quovis casu, siquidem ad usum nostrum rite adhibeatur, determinato terminorum numero constat.

§ 11. Si enim ope formulae nostrae primum exhibitae

$$\begin{aligned}\int n = \; & \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) - \int(n-22) \\ & - \int(n-26) + \int(n-35) + \int(n-40) - \int(n-51) - \int(n-57) + \int(n-70) + \int(n-77) \\ & - \int(n-92) - \int(n-100) + \text{etc.}\end{aligned}$$

summam divisorum numeri n invenire velimus ex cognitis divisorum summis numerorum minorum, plures terminos hujus formulae accipere non oportet, quam quoad ad summas divisorum numerorum negativorum perveniatur. Omnes scilicet termini, qui post signum $\int$ numeros negativos continent, sunt rejiciendi; unde patet si n sit numerus exiguus, paucissimos terminos sufficere, quo major autem fuerit numerus n, eo plures terminos ex formula nostra generali ad usum adhiberi debere.

§ 12. Summa igitur divisorum numeri propositi n ex summis divisorum aliquot numerorum minorum, quas cognitas esse assumo, conflatur; quoniam quovis casu summae numerorum negativorum rejiciuntur. Quae cautio cum eo sit facilior, quod numerorum negativorum summa divisorum ne concipi quidem possit, insuper moneri oportet, quomodo operatio sit dirigenda iis casibus, quibus formula nostra praebet terminum $\int(n-n)$ seu $\int 0$, qui cum cyphra per omnes numeros sit divisibilis, vel infinitus, vel indeterminatus videtur. Casus hic autem toties occurrit, quoties n est numerus ex serie numerorum pentagonalium vel ipsa, vel retro continuata; his igitur casibus tenendum est, semper pro termino $\int(n-n)$ seu $\int 0$ ipsum illum numerum n, qui proponitur, esse scribendum, et quidem cum eo signo, quo terminus $\int(n-n)$ in formula nostra afficitur.

§ 13. His expositis praeceptis, quae ad usum formulae nostrae observari debent, exempla a numeris minimis inchoando apponam, quo facilius vis formulae nostrae perspiciatur, simulque ejus veritas agnoscatur.

$\int 1 = \int 0$ seu
$\int 1 = 1 = 1$

$\int 2 = \int 1 + \int 0$ seu
$\int 2 = 1 + 2 = 3$

$\int 3 = \int 2 + \int 1$ seu
$\int 3 = 3 + 1 = 4$

$\int 4 = \int 3 + \int 2$ seu
$\int 4 = 4 + 3 = 7$

$\int 5 = \int 4 + \int 3 - \int 0$ seu
$\int 5 = 7 + 4 - 5 = 6$

$\int 6 = \int 5 + \int 4 - \int 1$ seu
$\int 6 = 6 + 7 - 1 = 12$

$\int 7 = \int 6 + \int 5 - \int 2 - \int 0$ seu
$\int 7 = 12 + 6 - 3 - 7 = 8$

$$\int 8 = \int 7 + \int 6 - \int 3 - \int 1 \quad \text{seu}$$
$$\int 8 = 8 + 12 - 4 - 1 = 15$$

$$\int 9 = \int 8 + \int 7 - \int 4 - \int 2 \quad \text{seu}$$
$$\int 9 = 15 + 8 - 7 - 3 = 13$$

$$\int 10 = \int 9 + \int 8 - \int 5 - \int 3 \quad \text{seu}$$
$$\int 10 = 13 + 15 - 6 - 4 = 18$$

$$\int 11 = \int 10 + \int 9 - \int 6 - \int 4 \quad \text{seu}$$
$$\int 11 = 18 + 13 - 12 - 7 = 12$$

$$\int 12 = \int 11 + \int 10 - \int 7 - \int 5 + \int 0 \quad \text{seu}$$
$$\int 12 = 12 + 18 - 8 - 6 + 12 = 28.$$

§ 14. Exempla haec attentius inspicienti, atque etiam ad numeros majores progredienti, non sine admiratione patebit, quemadmodum semper quasi praeter expectationem ad veram divisorum summam numeri propositi perveniatur; et quo hic consensus facilius deprehendatur, supra jam omnium numerorum centenario non majorum summas divisorum exhibui; unde veritas nostrae formulae in numeris majoribus explorari poterit. Imprimis autem non sine delectatione reperiemus, quoties numerus propositus fuerit primus, ex formula nostra pro ejus divisorum summa inveniri numerum unitate majorem. Evolvamus in hunc finem exemplum, quo numerus propositus $n = 101$, quasi ignorantes exploraturi, utrum hic numerus sit primus nec ne? atque operatio ita constabit:

$$\begin{aligned}\int 101 = {} & \int 100 + \int 99 - \int 96 - \int 94 + \int 89 + \int 86 - \int 79 - \int 75 \\ & 217 + 156 - 252 - 144 + 90 + 132 - 80 - 124 \\ & + \int 66 + \int 61 - \int 50 - \int 44 + \int 31 + \int 24 - \int 9 - \int 1 \\ & + 144 + 62 - 93 - 84 + 32 + 60 - 13 - 1.\end{aligned}$$

Colligendis ergo binis terminis erit

$$\begin{aligned}\int 101 = {} & + 373 - 396 \\ & + 222 - 204 \\ & + 206 - 177 \\ & + 92 - 14 \\ \text{seu } \int 101 = {} & + 893 - 791 = 102.\end{aligned}$$

Reperitur ergo summa divisorum numeri 101 unitae major scilicet 102, unde, etiamsi id aliunde non constaret, sequitur manifesto, numerum 101 esse primum. Hoc autem merito eo mirabilius videtur, cum nulla operatio sit instituta, quae ad rationem divisorum ullo modo referri queat; quin etiam divisores, quorum summa per hanc regulam reperitur, ipsi manent incogniti, etiamsi saepe ex consideratione ipsius summae concludi possint.

§ 15. Insignis haec proprietas, qua summae divisorum sunt praeditae, non minus foret memorabilis, etiamsi ejus demonstratio esset obvia et quasi in aprico posita. Sin autem demonstratio admodum esset abstrusa, atque numerorum proprietatibus maxime reconditis inniteretur, inde non mediocriter certe pretium hujus legis progressionis repertae augeretur, siquidem earum veritatum

investigatio eo magis est laudanda, quo magis eae fuerint absconditae. Verum dum fateri cogor, me non solum nullam hujus veritatis demonstrationem proferre posse, sed etiam propemodum pro desperato habere, nescio an non ob hanc ipsam causam cognitio talis veritatis multo magis sit aestimanda, cujus demonstratio nobis est imperscrutabilis. Atque hanc ob rem istam veritatem pluribus exemplis confirmare visum est, quod mihi quidem ejus demonstrationem exhibere non liceat.

§ 16. Eximium igitur hic ejusmodi propositionum habemus exemplum, de quarum veritate nullo modo dubitare possumus, etiamsi eas demonstrare non valeamus, quod plerisque eo magis mirum videbitur, quod in mathesi vulgo nullae aliae propositiones admitti putantur, nisi quarum veritas ex indubitatis principiis evinci queat. Interim tamen non fortuito et quasi divinando ad cognitionem hujus veritatis perveni; cui enim in mentem venire potuisset, ordinem, qui forte in summis divisorum locum habuerit, ex natura serierum recurrentium ac numerorum pentagonalium per solam conjecturam elicere velle? Hanc ob rem non abs re fore arbitror, si modum, quo ad cognitionem hujus ordinis pertigerim, dilucide exposuero, praesertim cum is admodum sit reconditus ac longe multasque per ambages conquisitus.

§ 17. Deductus autem sum ad hanc observationem per considerationem istius formulae infinitae

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)(1-x^8) \text{ etc.},$$

cujus valorem, si multiplicatione singulorum factorum actu instituta evolvatur, ac secundum potestates ipsius x disponatur, deprehendi in sequentem seriem converti:

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + x^{57} - \text{etc.},$$

ubi in exponentibus ipsius x iidem numeri occurrunt quos supra descripsi, numeri scilicet pentagonales cum ipsi, tum retro continuati. Unde, quo ordo facilius perspiciatur, haec series ita exhiberi poterit, ut utrinque in infinitum excurrat:

$$s = \text{etc.} + x^{26} - x^{15} + x^7 - x^2 + x^0 - x^1 + x^5 - x^{12} + x^{22} - x^{35} + x^{51} - \text{etc.}$$

§ 18. Aequalitas harum duarum formularum pro s exhibitarum jam est id ipsum, quod solida demonstratione confirmare non possum; verum tamen, qui opus evolutionis formulae prioris

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5) \text{ etc.}$$

in se suscipere, hosque factores successive in se multiplicare voluerit, statim ad terminos priores alterius seriei $s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \text{etc.}$ perveniet, neque difficulter perspiciet, bina signa + et — geminata se invicem excipere, et exponentes potestatum ipsius x eam legem sequi, quam jam satis exposui. Concessa autem hac aequalitate inter binas istas formulas infinitas, proprietas summarum divisorum, quam ante indicavi, rigide inde demonstrari potest; atque vicissim, si haec proprietas pro vera agnoscatur, ex ea veritas consensus duarum harum formularum evincetur.

§ 19. Quodsi enim pro demonstrato assumamus, posito

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5) \text{ etc.}$$

$$\text{fore} \quad s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}$$

erit logarithmis sumendis

$$ls = l(1-x) + l(1-x^2) + l(1-x^3) + l(1-x^4) + l(1-x^5) + \text{etc.}$$

$$\text{et} \quad ls = l(1 - x - xx + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}).$$

Sumantur utriusque formae differentialia, eritque

$$\frac{ds}{s} = \frac{-dx}{1-x} - \frac{2xdx}{1-xx} - \frac{3xxdx}{1-x^3} - \frac{4x^3dx}{1-x^4} - \frac{5x^4dx}{1-x^5} \text{ etc.}$$

$$\text{et} \quad \frac{ds}{s} = \frac{-dx - 2xdx + 5x^4dx + 7x^6dx - 12x^{11}dx - 15x^{14}dx + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}}.$$

Multiplicetur utraque per $\frac{-x}{dx}$, ut habeatur

$$\text{I.} \quad -\frac{xds}{sdx} = \frac{x}{1-x} + \frac{2x^2}{1-xx} + \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \frac{5x^5}{1-x^5} + \text{ etc.}$$

$$\text{II.} \quad -\frac{xds}{sdx} = \frac{x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - 26x^{26} + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}}.$$

§ 20. Harum expressionum inter se aequalium contemplemur primo priorem, ac singulos terminos more consueto in progressiones geometricas convertamus; quo facto prodibit, infinitas has progressiones geometricas secundum potestates ipsius x disponendo:

$-\frac{xds}{sdx} =$	$+x^1$	$+x^2$	$+x^3$	$+x^4$	$+x^5$	$+x^6$	$+x^7$	$+x^8$	$+x^9$	$+x^{10}$	$+x^{11}$	$+x^{12}$ etc.
		+2	. .	+2	. .	+2	. .	+2	. .	+2	. .	+2
			+3	. .	. .	+3	. .	. .	+3	. .	. .	+3
				+4	. .	. .	. .	+4	. .	. .	. .	+4
					+5	. .	. .	. .	. .	+5	. .	. .
						+6	. .	. .	. .	. .	. .	+6
							+7	. .	. .	. .	. .	. .
								+8	. .	. .	. .	. .
									+9	. .	. .	. .
										+10	. .	. .
											+11	. .
												+12

§ 21. Si jam singularum potestatum ipsius x coefficientes colligantur, habebitur:

$$-\frac{xds}{sdx} = x^1 + x^2(1+2) + x^3(1+3) + x^4(1+2+4) + x^5(1+5) + x^6(1+2+3+6) + \text{etc.}$$

ubi manifestum est, cujusque potestatis ipsius x coefficientem esse aggregatum omnium numerorum, per quos exponens illius potestatis est divisibilis. Scilicet potestatis x^n coefficiens erit summa omnium divisorum numeri n; erit ergo is secundum modum signandi supra receptum $= \int n$. Hinc itaque seriei ipsi $-\frac{xds}{sdx}$ aequalis inventa ita exhibebitur, ut sit

$$-\frac{xds}{sdx} = x\int 1 + x^2\int 2 + x^3\int 3 + x^4\int 4 + x^5\int 5 + x^6\int 6 + x^7\int 7 + \text{etc.}$$

sicque posito $x = 1$, prodit progressio summarum divisorum, qui singulis numeris ordine naturali progredientibus conveniunt.

§ 22. Designemus jam hanc seriem per t, ut sit

$$t = x^1\int 1 + x^2\int 2 + x^3\int 3 + x^4\int 4 + x^5\int 5 + x^6\int 6 + x^7\int 7 + \text{etc.}$$

et ob $t = -\frac{xds}{sdx}$, erit quoque

$$t = \frac{x^1 + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - 26x^{26} + \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}}.$$

Necesse igitur est, ut ex evolutione hujus fractionis pro t series obtineatur aequalis illi, quam prior forma suppeditavit, unde manifestum est, seriem illam pro t inventam esse recurrentem, cujus singuli termini per praecedentes determinentur, secundum scalam relationis, quam denominator $1 - x - x^2 + x^5 + x^7$ etc. indicat.

§ 23. Quo nunc facilius indoles hujus seriei recurrentis cognoscatur, binos istos valores pro t inventos inter se coaequemus, atque ad fractionem tollendam uterque per denominatorem

$$1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \text{etc.}$$

multiplicetur, quo facto orietur, terminis secundum potestates ipsius x disponendis:

$$\begin{array}{cccccccccccc}
x^1\int 1 & +x^2\int 2 & +x^3\int 3 & +x^4\int 4 & +x^5\int 5 & +x^6\int 6 & +x^7\int 7 & +x^8\int 8 & +x^9\int 9 & +x^{10}\int 10 & +x^{11}\int 11 & +x^{12}\int 12 \text{ etc.} \\
 & -\int 1 & -\int 2 & -\int 3 & -\int 4 & -\int 5 & -\int 6 & -\int 7 & -\int 8 & -\int 9 & -\int 10 & -\int 11 \\
 & & -\int 1 & -\int 2 & -\int 3 & -\int 4 & -\int 5 & -\int 6 & -\int 7 & -\int 8 & -\int 9 & -\int 10 \\
 & & & & & +\int 1 & +\int 2 & +\int 3 & +\int 4 & +\int 5 & +\int 6 & +\int 7 \\
 & & & & & & & +\int 1 & +\int 2 & +\int 3 & +\int 4 & +\int 5 \text{ etc.}
\end{array}$$

aequale

$$x^1 \quad +2x^2 \quad * \quad * \quad -5x^5 \quad * \quad -7x^7 \quad * \quad * \quad * \quad * \quad +12x^{12} \text{ etc.}$$

§ 24. Cum jam singularum potestatum ipsius x coefficientes se mutuo destruere debeant, hinc sequentes eliciemus aequalitates:

$$\begin{array}{l|l}
\int 1 = 1 & \int 7 = \int 6 + \int 5 - \int 2 - 7 \\
\int 2 = \int 1 + 2 & \int 8 = \int 7 + \int 6 - \int 3 - \int 1 \\
\int 3 = \int 2 + \int 1 & \int 9 = \int 8 + \int 7 - \int 4 - \int 2 \\
\int 4 = \int 3 + \int 2 & \int 10 = \int 9 + \int 8 - \int 5 - \int 3 \\
\int 5 = \int 4 + \int 3 - 5 & \int 11 = \int 10 + \int 9 - \int 6 - \int 4 \\
\int 6 = \int 5 + \int 4 - \int 1 & \int 12 = \int 11 + \int 10 - \int 7 - \int 5 + 12
\end{array}$$

etc.

quae manifesto redeunt ad istas:

$$\begin{array}{l|l}
\int 1 = 1 & \int 7 = \int(7-1) + \int(7-2) - \int(7-5) - 7 \\
\int 2 = \int(2-1) + 2 & \int 8 = \int(8-1) + \int(8-2) - \int(8-5) - \int(8-7) \\
\int 3 = \int(3-1) + \int(3-2) & \int 9 = \int(9-1) + \int(9-2) - \int(9-5) - \int(9-7) \\
\int 4 = \int(4-1) + \int(4-2) & \int 10 = \int(10-1) + \int(10-2) - \int(10-5) - \int(10-7) \\
\int 5 = \int(5-1) + \int(5-2) - 5 & \int 11 = \int(11-1) + \int(11-2) - \int(11-5) - \int(11-7) \\
\int 6 = \int(6-1) + \int(6-2) - \int(6-5) & \int 12 = \int(12-1) + \int(12-2) - \int(12-5) - \int(12-7) + 12.
\end{array}$$

§ 25. Hic perspicuum est, numeros, qui continuo a numero proposito, cujus divisorum summa quaeritur, subtrahi debent, esse ipsos numeros seriei 1, 2, 5, 7, 12, 15, 22, 26, etc., ex quibus tot quovis casu sunt sumendi, quoad numerum propositum non excedant: atque etiam signa eam tenere rationem, quae supra est descripta. Hinc ergo proposito numero quocunque n manifestum est,

fore $\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) -$ etc., hos terminos eousque continuando, donec numeri signum $\int$ praefixum habentes, fiant negativi. Simul ergo ex origine seriei hujus recurrentis ratio patet, cur ista progressio quovis casu ulterius continuari non debeat.

§ 26. Quod porro ad numeros absolutos attinet, qui in formularum inventarum aliquibus sub finem annectuntur, manifestum est, eos ex numeratore fractionis, qua valor ipsius t expressus est inventus (§ 22) oriri, atque iis tantum casibus legem continuitatis interrumpere, quibus numerus n est terminus hujus seriei 1, 2, 5, 7, 12, 15, 22, 26, etc. quanquam ne hoc quidem casu lex signorum perturbatur. His autem casibus numerus absolutus insuper cum signo suo adjiciendus ipsi numero proposito est aequalis; atque si legem ante descriptam consideremus, hunc numerum utique deprehendemus respondere termino $\int(n-n)$: unde ratio patet, cur quoties in applicatione formae

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \text{etc.}$$

pervenitur ad terminum $\int(n-n)$, is non omitti, sed pro ejus valore ipse numerus n scribi debeat. Hinc igitur regula supra exposita in omnibus partibus confirmatur.



XII.

De numeris, qui sunt aggregata duorum quadratorum.

(N. Comment. IV. 1752 — 53. p. 3.)

§ 1. Naturam numerorum pluribus modis scrutari solent arithmetici, dum eorum originem vel per additionem, vel per multiplicationem repraesentant. Prioris generis sine dubio simplicissima est compositio ex unitatibus, qua omnes numeri integri per aggregationem unitatum oriri concipiuntur. Tum numeri quoque ita considerari possunt, prouti ex additione duorum pluriumve aliorum numerorum integrorum nascuntur, quo pertinet problema de partitione numerorum, cujus solutionem aliquot abhinc annis exposui, in quo quaeritur, quot variis modis quilibet numerus propositus per additionem duorum pluriumve numerorum minorum resultare possit (*). Hic autem constitui eam numerorum compositionem perpendere, qua per additionem duorum quadratorum prodeunt; et cum hoc modo non omnes numeri oriantur, quoniam ingens est eorum multitudo, qui per additionem duorum quadratorum produci nequeunt, in eorum naturam et proprietates, qui sunt summae duorum quadratorum, hic inquiram. Quarum proprietatum etiamsi pleraeque jam sint cognitae, et quasi per inductionem erutae, tamen firmis demonstrationibus maximam partem destituuntur: quarum veritati cum haud contemnenda pars analyseos Diophanteae innitatur, in hac dissertatione plurium hujusmodi propositionum, quae adhuc sine demonstrationibus sunt admissae, demonstrationes adornabo, simul vero etiam eas commemorabo, quas mihi quidem etiamnunc demonstrare non licuit, etiamsi de earum veritate nullo modo dubitare queamus.

§ 2. Primum igitur cum numeri quadrati sint: 0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, etc. istos numeros qui ex combinatione binorum quadratorum oriuntur, inspexisse juvabit, quos propterea usque ad 200 hic apponam:

0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100, 101, 104, 106, 109, 113, 116, 117, 121, 122, 125, 128, 130, 136, 137, 144, 145, 146, 148, 149, 153, 157, 160, 162, 164, 169, 170, 173, 178, 180, 181, 185, 193, 194, 196, 197, 200 etc.

Hi nempe omnes sunt numeri usque ad 200, qui ex additione duorum quadratorum proveniunt: hosque numeros cum omnibus in infinitum sequentibus vocabo summas duorum quadratorum, quos idcirco in hac formula generali $xx + yy$ comprehendi manifestum est, dum pro x et y successive omnes numeri integri 0, 1, 2, 3, 4, 5, 6 etc. substituuntur. Qui igitur numeri in his non reperiuntur, ii non sunt summae duorum quadratorum, qui ergo sunt usque ad 200:

3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38, 39, 42, 43, 44, 46, 47, 48, 51, 54, 55, 56, 57, 59, 60, 62, 63, 66, 67, 69, 70, 71, 75, 76, 77, 78, 79, 83, 84, 86, 87, 88, 91, 92, 93, 94, 95, 96, 99, 102, 103, 105, 107, 108, 110, 111, 112, 114, 115,

(*) Vide supra comment. IX. pag. 73 seqq.

118, 119, 120, 123, 124, 126, 127, 129, 131, 132, 133, 134, 135, 138, 139, 140, 141, 142, 143, 147, 150, 151, 152, 154, 155, 156, 158, 159, 161, 163, 165, 166, 167, 168, 171, 172, 174, 175, 176, 177, 179, 182, 183, 184, 186, 187, 188, 189, 190, 191, 192, 195, 198, 199 etc. Unde patet saltem usque ad 200 multitudinem numerorum, qui non sunt summae duorum quadratorum, majorem esse quam eorum, qui sunt summae duorum quadratorum. Ceterum inspicienti statim patebit neutram istorum numerorum seriem certa et assignabili lege contineri, atque ob hoc ipsum difficilius erit utriusque indolem investigare.

§ 3. Cum omnis numerus quadratus sit vel par, hocque casu per 4 divisibilis et in hac forma $4a$ contentus, vel impar, hocque casu in hac forma $8b+1$ contineatur: omnis numerus ex duobus quadratis compositus erit, vel primo, summa duorum quadratorum parium, et ad hanc formam $4a+4b$ pertinebit; eritque ergo per 4 divisibilis;

vel secundo, summa duorum quadratorum alterius paris alterius imparis, et propterea in hujusmodi forma $4a+8b+1$, seu in hac $4a+1$ continebitur, unitate ergo excedet multiplum quaternarii;

vel tertio, summa duorum quadratorum imparium, eritque idcirco hujus formae

$$8a+1+8b+1,$$

seu in hac $8a+2$ continebitur. Erit scilicet numerus impariter par et binario excedet multiplum octonarii.

Quia ergo omnes numeri impares vel unitate excedunt multiplum quaternarii, seu hujus sunt formae $4n+1$, vel unitate deficiunt a multiplo quaternarii; seu hujus sunt formae $4n-1$; patet nullos numeros impares hujus posterioris formae $4n-1$ esse summas duorum quadratorum, seu ex serie numerorum, qui sunt summae duorum quadratorum excluduntur omnes numeri in hac forma contenti $4n-1$.

Deinde quia omnes numeri impariter pares vel binario superant multiplum octonarii, ut sint $8n+2$, vel binario deficiunt a multiplo octonarii, ut sint $8n-2$, patet nullos numeros hujus posterioris formae esse summas duorum quadratorum, sicque ex serie numerorum, qui sunt summae duorum quadratorum, excluduntur numeri hujus formae $8n-2$.

Interim tamen probe observandum est neque omnes numeros in hac forma $4n+1$, neque in hac $8n+2$ contentos esse summas duorum quadratorum. Illius enim formae excluduntur numeri: 21, 33, 57, 69, 77, 93, 105, 129, etc. hujus vero isti: 42, 66, 114, 138, 154, etc., quorum ratio deinceps investigabitur.

§ 4. Interim tamen numeri, qui sunt summae duorum quadratorum, ita nexu quodam inter se conjunguntur, ut ex uno hujus indolis numero infiniti alii ejusdem naturae assignari queant. Quod quo facilius perspiciatur, sequentia lemmata, quae quidem vulgo satis sunt nota, adjungam.

I. **Si numerus p sit summa duorum quadratorum, erunt quoque numeri $4p$, $9p$, $16p$ et generatim nnp summae duorum quadratorum.**

Cum enim sit $p=aa+bb$, erit $4p=4aa+4bb$; $9p=9aa+9bb$; $16p=16aa+16bb$ et $nnp=nnaa+nnbb$, quae formulae sunt pariter summae duorum quadratorum.

II. Si numerus p sit summa duorum quadratorum, erit quoque $2p$, et generatim $2nnp$ summa duorum quadratorum.

Sit enim $p = aa + bb$, erit $2p = 2aa + 2bb$. Sed est $2aa + 2bb = (a+b)^2 + (a-b)^2$, unde erit $2p = (a+b)^2 + (a-b)^2$, ac propterea summa duorum quadratorum. Hinc vero porro erit $2nnp = nn(a+b)^2 + nn(a-b)^2$.

III. Si numerus par $2p$ fuerit summa duorum quadratorum, erit etiam ejus semissis p summa duorum quadratorum.

Sit enim $2p = aa + bb$, erit numerorum a et b uterque vel par, vel impar, unde utroque casu erit tam $\frac{a+b}{2}$ quam $\frac{a-b}{2}$ numerus integer. Est vero $aa + bb = 2\left(\frac{a+b}{2}\right)^2 + 2\left(\frac{a-b}{2}\right)^2$, quo valore substituto fit $p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$.

Hinc ergo omnes numeri pares, qui sunt summae duorum quadratorum, per continuam bisectionem tandem revocantur ad numeros impares ejusdem indolis. Quare vicissim, si soli numeri impares, qui sunt summae duorum quadratorum, cognoscantur, ex iis omnes quoque pares per continuam duplicationem derivabuntur.

§ 5. Deinde notatu dignum est sequens theorema, quo natura numerorum, qui sunt summae duorum quadratorum, non mediocriter illustratur.

Theorema. *Si* p *et* q *sint duo numeri, quorum uterque est summa duorum quadratorum, erit etiam eorum productum* pq *summa duorum quadratorum.*

Demonstratio. Sit $p = aa + bb$ et $q = cc + dd$, erit

$$pq = (aa + bb)(cc + dd) = aacc + aadd + bbcc + bbdd:$$

quae expressio hoc modo repraesentari potest, ut sit:

$$pq = aacc + 2abcd + bbdd + aadd - 2abcd + bbcc,$$

ideoque $pq = (ac + bd)^2 + (ad - bc)^2$: unde productum pq erit summa duorum quadratorum. Q. E. D.

Ex hac propositione sequitur, quomodocunque plures numeri, qui singuli sint summae duorum quadratorum, invicem multiplicentur, producta semper esse summas duorum quadratorum. Atque ex forma generali tradita patet, productum ex duobus hujusmodi numeris duplici modo in duo quadrata resolvi posse: si enim sit $p = aa + bb$, et $q = cc + dd$, erit tam $pq = (ac + bd)^2 + (ad - bc)^2$, quam $pq = (ac - bd)^2 + (ad + bc)^2$, quae formulae erunt diversae, nisi sit, vel $a = b$, vel $c = d$. Sic cum sit $5 = 1 + 4$, et $13 = 4 + 9$, productum $5.13 = 65$ duplici modo erit summa duorum quadratorum, scilicet erit

$$65 = (1.3 + 2.2)^2 + (2.3 - 1.2)^2 = 49 + 16, \text{ et } 65 = (2.2 - 1.3)^2 + (2.3 + 1.2)^2 = 1 + 64.$$

Atque si productum habeatur ex pluribus numeris, qui singuli sint summae duorum quadratorum, id pluribus modis in duo quadrata resolvi poterit. Uti si proponatur numerus $1105 = 5.13.17$, ejus resolutiones in duo quadrata erunt hae:

$$1105 = 33^2 + 4^2 = 32^2 + 9^2 = 31^2 + 12^2 = 24^2 + 23^2.$$

Quatuor scilicet hic resolutiones locum habent.

§ 6. Quanquam autem ita evictum est, si factores p et q sint summae duorum quadratorum, etiam fore productum pq summam duorum quadratorum; tamen hujus propositionis conversa hinc

non sequitur, ut, si productum sit duorum quadratorum summa, etiam ejus factores sint numeri ejusdem naturae, neque enim hanc conclusionem regulae logicae, neque ipsa rei natura probarent. Nam numerus $45 = 36 + 9$ est summa duorum quadratorum, interim tamen horum factorum ejus 3, 15 neuter est summa duorum quadratorum. Magis autem firma videtur haec conclusio: si productum pq, et alteruter ejus factor p fuerint duorum quadratorum summae, alterum quoque factorem q fore summam duorum quadratorum. Tametsi autem haec conclusio forte sit vera, regulis tamen ratiocinandi non confirmatur, neque enim cum demonstratum sit, si producti pq bini factores p et q sint duorum quadratorum summae, ipsum pq fore summam duorum quadratorum, hinc legitima consequentia inferri potest: si et productum pq, et alter factor p, sint summae duorum quadratorum, etiam alterum factorem q fore summam duorum quadratorum. Hujusmodi enim consequentiam non esse legitimam, vel hoc exemplum evidenter evincet: certum est si bini factores p et q sint numeri pares, etiam productum pq fore numerum parem; si quis autem hinc concludere velit, si productum pq et alter factor p sint numeri pares, etiam alterum factorem q fore parem, is vehementer falleretur.

§ 7. Quare si verum sit, ut, cum productum pq et alter ejus factor p fuerint summae duorum quadratorum, alter quoque factor q sit summa duorum quadratorum, haec propositio non ex ante demonstrata potest inferri, sed peculiari demonstratione muniri debet. Haec autem demonstratio non tam plana est, quam praecedens, et non nisi per plures ambages concinnari potest; ac demonstratio quidem, quam inveni, ita comparata videtur, ut non mediocrem vim ratiocinii requirat. Hanc ob rem propositiones, ex quibus tandem non solum haec veritas conficitur, sed etiam aliae insignes proprietates hujusmodi numerorum, qui sunt summae duorum quadratorum, cognoscuntur, cum suis demonstrationibus hic ordine proponam, operamque dabo, ut nihil quicquam in rigore demonstrandi desiderari queat. Iis autem, quae hactenus de his numeris praemisi, uti sunt trivia et in vulgus nota, ita instar lemmatum in sequentibus demonstrationibus utar.

§ 8. **Propositio I.** *Si productum* pq *sit summa duorum quadratorum, et alter factor* p *sit numerus primus, pariterque duorum quadratorum summa, erit quoque alter factor* q *summa duorum quadratorum.*

Demonstratio. Sit $pq = aa + bb$, et $p = cc + dd$; quia p est numerus primus, erunt c et d numeri inter se primi. Erit itaque $q = \frac{aa + bb}{cc + dd}$, et propterea, ob q numerum integrum, numerator $aa + bb$ per denominatorem $cc + dd$ erit divisibilis. Hinc quoque per $cc + dd$ divisibilis erit numerus $cc(aa + bb) = aacc + bbcc$; at cum etiam hic numerus $aa(cc + dd) = aacc + aadd$ per $cc + dd$ sit divisibilis, horum numerorum differentia $aacc + bbcc - aacc - aadd$ seu $bbcc - aadd$ per $cc + dd$ divisibilis sit necesse est. Cum autem sit $cc + dd$ numerus primus, et $bbcc - aadd$ factores habeat $bc + ad$ et $bc - ad$, alteruter horum factorum, nempe $bc \pm ad$ per $cc + dd$ erit divisibilis. Sit itaque $bc \pm ad = mcc + mdd$: quicunque autem numeri sint a et b, ii ita exprimi possunt, ut sit $b = mc + x$, et $a = \pm md + y$, existentibus x et y numeris integris sive affirmativis sive negativis. His vero valoribus pro b et a substitutis aequatio $bc \pm ad = mcc + mdd$ induet hanc formam: $mcc + cx + mdd \pm dy = mcc + mdd$, seu $cx \pm dy = 0$. Hinc erit $\frac{x}{y} = \mp \frac{d}{c}$,

et quia d et c sunt numeri primi inter se, necesse est, ut sit $x = nd$ et $y = \mp nc$, unde habebitur $a = \pm md \mp nc$ et $b = mc + nd$, hujusmodi scilicet valores habere debebunt numeri a et b, ut numerus $pq = aa + bb$ sit divisibilis per numerum primum $p = cc + dd$. Verum istis valoribus pro a et b substitutis fiet:

$$pq = mmdd - 2mncd + nncc + mmcc + 2mncd + nndd, \quad \text{seu} \quad pq = (mm + nn)(cc + dd).$$

Jam ob $p = cc + dd$, erit $q = mm + nn$; ideoque si productum pq fuerit summa duorum quadratorum $aa + bb$, et alter factor p sit numerus primus pariterque duorum quadratorum summa $cc + dd$, necessario sequitur etiam alterum factorem q fore summam duorum quadratorum. Q. E. D.

§ 9. **Coroll. 1.** Si ergo summa duorum quadratorum divisibilis sit per numerum primum, qui ipse sit summa duorum quadratorum, etiam quotus ex divisione resultans erit summa duorum quadratorum. Ita si summa duorum quadratorum fuerit divisibilis per quempiam ex his numeris primis 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc. quotus semper erit summa duorum quadratorum.

§ 10. **Coroll. 2.** Si ergo litterae α, β, γ, δ, etc. denotent hujusmodi numeros primos, qui sunt summae duorum quadratorum; hinc patet, si productum αq sit summa duorum quadratorum, fore etiam factorem q summam duorum quadratorum.

§ 11. **Coroll. 3.** Hinc autem porro facile colligitur, si productum $\alpha\beta q$ fuerit summa duorum quadratorum, fore etiam factorem q summam duorum quadratorum. Cum enim sit $\alpha\beta q$ summa duorum quadratorum, per corollarium praecedens erit quoque βq summa duorum quadratorum, et ob eandem rationem erit quoque q summa duorum quadratorum.

§ 12. **Coroll. 4.** Simili modo evidens est, si productum $\alpha\beta\gamma\delta\epsilon q$ fuerit summa duorum quadratorum, tum quoque factorem q esse summam duorum quadratorum; hinc si productum pq sit summa duorum quadratorum, ejusque factor p productum ex quotcunque numeris primis, quorum singuli sint summae duorum quadratorum, fore etiam alterum factorem q summam duorum quadratorum.

§ 13. **Schollon.** Regulae logicae non permittunt, ut haec propositio ita convertatur, ut, quoties alter factor q sit summa duorum quadratorum, etiam alter factor p pronunciari possit, vel summa duorum quadratorum, si est primus, vel productum ex numeris primis, qui singuli sint summae duorum quadratorum. De hoc ipso enim nondum constat, utrum productum ex aliquot numeris primis, qui ipsi non sint summae duorum quadratorum, nequeat esse summa duorum quadratorum; quin potius contrario jam habemus casum, quo productum $45 = 3.3.5$ est summa duorum quadratorum, cum tamen ejus factores 3 et 3 non sint hujus indolis. Verum propositio corollarii ultimi ita converti potest, ut a negatione consequentis recte ad negationem antecedentis concludatur, quam conversionem utpote maximi momenti in hac propositione complectar.

§ 14. **Propositio II.** *Si productum* pq *sit summa duorum quadratorum, ejus factor autem* q *non sit summa duorum quadratorum, tum alter factor* p, *si sit numerus primus, non erit summa duorum quadratorum, sin autem non sit primus, saltem factorem certe habebit primum, qui non sit summa duorum quadratorum.*

Demonstratio. Cum alter factor p sit vel numerus primus, vel compositus, utrumque casum seorsim perpendere convenit. Sit primo p numerus primus; cum igitur si esset summa duorum quadratorum, quoque alter factor q foret summa duorum quadratorum; quod cum hypothesi adversetur, sequitur, factorem p non esse summam duorum quadratorum. Sit secundo p numerus compositus; et ex praecedentibus liquet, si omnes ejus factores primi essent summae duorum quadratorum, etiam alterum factorem q ejusdem fore indolis. Quare cum, per hypothesin, q non sit summa duorum quadratorum, sequitur, non omnes factores ipsius p esse summas duorum quadratorum. Q. E. D.

§ 15. **Coroll. 1.** Si igitur productum pq sit summa duorum quadratorum, ejus tamen alter factor q in duo quadrata sit irresolubilis, alter factor p, vel ipse non erit summa duorum quadratorum, vel saltem factorem habebit primum in duo quadrata irresolubilem. Uti si sit $pq = 45$ et $q = 3$, erit $p = 15$ et factorem habet 3, qui non est summa duorum quadratorum.

§ 16. **Coroll. 2.** Hinc autem nondum concludere licet, alterum factorem p planè non esse summam duorum quadratorum, quamvis enim hoc certum sit casu, quo p est numerus primus, tamen id nondum constat casu, quo p est numerus compositus; quia p habere posset factorem in duo quadrata irresolubilem, etiamsi ipse numerus p esset summa duorum quadratorum.

§ 17. **Coroll. 3.** Hoc autem colligere licet: si p esset summa duorum quadratorum, tum non solum unum, sed ad minimum duos habere debere factores primos in duo quadrata irresolubiles. Sit enim $p = \alpha\beta\gamma\delta$, et δ factor ille in duo quadrata irresolubilis; perspicuum est, si p esset summa duorum quadratorum, deleto factore δ, insuper factorem residuum $\alpha\beta\gamma$ factorem in duo quadrata irresolubilem habere debere.

§ 18. **Scholion.** Cum de divisoribus numerorum, qui sunt summae duorum quadratorum, quaestio instituitur, circa quadratorum summam $aa + bb$, casus hi probe sunt distinguendi, utrum haec quadrata aa et bb, seu eorum radices a et b sint numeri primi inter se nec ne? Si enim a et b non sint numeri primi inter se, sed habeant communem divisorem n, ut sit $a = nc$ et $b = nd$, summa quadratorum erit $nncc + nndd = nn(cc + dd)$, ac propterea divisorem habebit n, hoc est, numerum quemcunque. Sin autem radices a et b fuerint numeri primi inter se, tum summa quadratorum $aa + bb$ plures numeros pro divisoribus non admittet: evidens enim est hujusmodi summam duorum quadratorum $aa + bb$ nunquam per 3 esse divisibilem. Nam quia per hypothesin utrumque quadratum seorsim non est per 3 divisibile, cum alioquin non forent prima inter se; si summa $aa + bb$ esset per 3 divisibilis, neutrum foret per 3 divisibile. Utriusque ergo radices futurae essent, vel hujus formae $3m + 1$, vel hujus $3m - 1$; sed summa hujusmodi duorum quadratorum, per 3 divisa, semper residuum 2 relinquit, ideoque per 3 nunquam est divisibilis. Eodem modo intelligitur, summam duorum quadratorum inter se primorum $aa + bb$ nunquam esse per 7, vel 11, vel 19 etc. divisibilem. Quinam autem sint in genere hi numeri, qui nunquam summae duorum quadratorum inter se primorum divisores existere queant, hoc modo non facile definitur. Demonstrari igitur convenit propositionem alias quidem satis notam, summam duorum quadratorum inter se primorum alios divisores primos non admittere, nisi qui ipsi sint summae duorum quadratorum. Praemitti autem debet sequens propositio.

§ 19. **Propositio III.** *Si summa duorum quadratorum inter se primorum* $aa + bb$ *divisibilis sit per numerum* p, *semper exhiberi poterit summa duorum aliorum quadratorum* $cc + dd$ *divisibilis per eundem numerum* p, *ita ut ista summa* $cc + dd$ *non sit major quam* $\frac{1}{2}pp$.

Demonstratio. Sit summa duorum quadratorum inter se primorum $aa + bb$ divisibilis per numerum p, et a et b numeri quantumvis magni. Quia ergo neque a neque b seorsim per p divisibilis est, numeri a et b ita exprimi poterunt, ut sit $a = mp \pm c$ et $b = np \pm d$, ubi numeros m et n ita determinare licet, ut c et d non excedant semissem ipsius p. Erit ergo

$$aa + bb = mmpp \pm 2mcp + cc + nnpp \pm 2ndp + dd,$$

quae formula cum et tota divisibilis sit per p (per hypothesin) et ejus pars $mmpp \pm 2mcp + nnpp \pm 2ndp$ per se divisorem habeat p, necesse est, ut altera pars $cc + dd$, quae est summa duorum quadratorum, itidem per p sit divisibilis. At cum radices c et d non excedant semissem ipsius p, summa quadratorum $cc + dd$ non excedet quadratum $\frac{1}{4}pp$ bis sumtum; ideoque summa duorum quadratorum $cc + dd$ exhiberi potest non major quam $\frac{1}{2}pp$, quae tamen sit per p divisibilis. Q. E. D.

§ 20. **Coroll. 1.** Si igitur non detur summa duorum quadratorum inter se primorum divisibilis per numerum p, quae non excedat $\frac{1}{2}pp$, nullae omnino dantur summae duorum quadratorum inter se primorum, quae per hunc numerum p essent divisibiles.

§ 21. **Coroll. 2.** Sic cum nulla detur summa duorum quadratorum inter se primorum infra $\frac{1}{2}.3^2$ seu infra $4\frac{1}{2}$, quae sit per 3 divisibilis, hinc luculenter sequitur, nullam omnino summam duorum quadratorum inter se primorum per 3 esse divisibilem. Similique modo pro numero 7, cum non detur summa duorum quadratorum infra $\frac{1}{2}.7^2 = 24\frac{1}{2}$ per 7 divisibilis, sequitur ne in maximis quidem numeris dari summas duorum quadratorum inter se primorum per 7 divisibiles.

§ 22. **Propositio IV.** *Summa duorum quadratorum inter se primorum dividi nequit per ullum numerum, qui ipse non sit summa duorum quadratorum.*

Demonstratio. Ad hoc demonstrandum ponamus summam duorum quadratorum inter se primorum $aa + bb$ divisibilem esse per numerum p, qui non sit summa duorum quadratorum. Exhiberi ergo posset alia summa duorum quadratorum inter se primorum $cc + dd$ non major quam $\frac{1}{2}pp$, quae esset divisibilis per p. Sit igitur $cc + dd = pq$, et cum p non sit summa duorum quadratorum, vel ipse numerus q non erit ejusmodi summa, vel saltem factorem habebit r, qui non erit summa duorum quadratorum. Quia vero $pq < \frac{1}{2}pp$, erit $q < \frac{1}{2}p$ et multo magis $r < \frac{1}{2}p$. Quare cum $cc + dd$ quoque divisibilis sit per $r < \frac{1}{2}p$, per propositionem praecedentem summa duorum quadratorum $ee + ff$ per eundem numerum r divisibilis exhiberi posset, quae non excederet $\frac{1}{2}rr$, neque multo magis $\frac{1}{8}pp$. Et cum r non sit summa duorum quadratorum, simili modo procedendo continuo ad minores summas duorum quadratorum deveniretur, quae per numerum non summam duorum quadratorum essent divisibiles. Quocirca cum in minimis numeris nulla detur summa duorum quadratorum inter se primorum, quae esset divisibilis per numerum, qui non sit summa duorum quadratorum, ne in maximis quidem numeris ejusmodi erunt summae duorum quadratorum, quae divisibiles sint per numeros, qui ipsi non essent summae duorum quadratorum. Q. E. D.

§ 23. **Coroll. 1.** Si ergo summa duorum quadratorum inter se primorum non fuerit numerus primus, omnes ejus factores primi quoque erunt summae duorum quadratorum. Quemadmodum igitur

productum ex quotcunque numeris primis, qui ipsi sunt summae duorum quadratorum, pariter est summa duorum quadratorum, ita nunc hujus propositionis conversa est demonstrata, ut summa duorum quadratorum (inter se primorum) per multiplicationem oriri nequeat, nisi ex numeris, qui ipsi sint summae duorum quadratorum.

§ 24. **Coroll. 2.** Omnes ergo numeri, qui sunt summae duorum quadratorum inter se primorum, vel ipsi in hac serie numerorum primorum continentur:

2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, etc.

vel ex duobus pluribusve numeris hujus seriei per multiplicationem componuntur. Omnes autem hi numeri primi praeter 2 unitate excedunt multiplum quaternarii, seu in hac forma $4n+1$ continentur.

§ 25. **Coroll. 3.** Si igitur summa duorum quadratorum $aa+bb$ divisibilis sit per numerum, qui non fuerit summa duorum quadratorum, hinc intelligetur quadrata illa aa et bb non esse inter se prima, neque adeo eorum radices a et b.

§ 26. **Coroll. 4.** Cum autem si $a=nc$ et $b=nd$ summa duorum quadratorum

$$aa+bb=nn(cc+dd)$$

per quemvis numerum n, qui non est summa duorum quadratorum, dividi possit, quoniam non solum per n, sed etiam per nn est divisibilis, evidens est, si summa duorum quadratorum divisibilis sit per quempiam numerum, qui non est summa duorum quadratorum, tum eam quoque per quadratum hujus numeri fore divisibilem. Sic cum $45=36+9$ sit divisibilis per 3, simul quoque divisibilis est per 9.

§ 27. **Coroll. 5.** Cum nullus numerorum in hac forma $4n-1$ contentorum sit summa duorum quadratorum, manifestum quoque est, nullam summam quadratorum inter se primorum dividi posse per ullum numerum primum, in forma $4n-1$ contentum, qui numeri primi sunt:

3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, etc.

§ 28. **Scholion.** Cum omnes numeri primi, qui sunt summae duorum quadratorum, excepto binario, hanc seriem constituant:

5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, etc.

qui non solum in hac forma $4n+1$ continentur, sed etiam, quantumvis ea longe continuetur, deprehendemus in ea omnes omnino numeros primos hujus formae $4n+1$ occurrere: unde per inductionem satis probabiliter concludere licet, nullum dari numerum primum formae $4n+1$, qui non simul sit summa duorum quadratorum. Interim tamen cum inductio quantumvis ampla vicem demonstrationis sustinere nequeat, hanc veritatem, quod omnis numerus primus formae $4n+1$ simul sit summa duorum quadratorum, etiamsi nemo agnoscere dubitet, tamen adhuc demonstratis matheseos veritatibus annumerare non licet. Fermatius quidem professus est, se ejus demonstrationem invenisse; quia autem eam nusquam publicavit, asserto quidem hujus profundissimi viri merito fidem adhibemus, istamque numerorum proprietatem credimus; haecque cognitio nostra mera fide sine scientia nititur. Quanquam autem ego multum in demonstratione eruenda frustra laboravi, tamen aliud argumentum pro hac veritate adstruenda reperi, quod etiamsi non summum rigorem sustineat, tamen cum inductione conjunctum demonstrationi pene rigorosae aequivalere videtur.

§ 28. **Propositio V.** *Omnis numerus primus, qui unitate excedit multiplum quaternarii, est summa duorum quadratorum.*

Tentamen Demonstrationis. Numeri primi, de quibus hic sermo est, in hac forma $4n+1$ continentur. Quodsi ergo numerus $4n+1$ fuerit primus, demonstravi per eum semper divisibilem esse hanc formam $a^{4n}-b^{4n}$, quicunque numeri pro a et b substituantur, dummodo neuter seorsim fuerit per $4n+1$ divisibilis. Cum autem sit $a^{4n}-b^{4n}=(a^{2n}-b^{2n})(a^{2n}+b^{2n})$, necesse est, ut alteruter factor, nempe vel $a^{2n}-b^{2n}$, vel $a^{2n}+b^{2n}$ sit divisibilis per numerum primum $4n+1$. Prout autem pro a et b alii atque alii numeri assumuntur, aliis casibus formula $a^{2n}-b^{2n}$, aliis vero formula $a^{2n}+b^{2n}$ erit per $4n+1$ divisibilis: unde assumere licet, etsi quidem hoc nondum firma demonstratione evincere valeo, semper ejusmodi numeros pro a et b assignari posse, ut formula $a^{2n}-b^{2n}$ non sit per $4n+1$ divisibilis: iis ergo casibus altera formula $a^{2n}+b^{2n}$ necessario per $4n+1$ erit divisibilis. Sit $a^n=p$ et $b^n=q$, habebiturque summa duorum quadratorum $pp+qq$ per $4n+1$ divisibilis, ita ut neutrum quadratum pp vel qq seorsim habeat divisorem $4n+1$. Ideoque etiamsi fortasse pp et qq communem habeant divisorem mm, ut sit

$$pp+qq=mm(rr+ss),$$

quia factor communis mm divisorem non habet $4n+1$, necesse est, ut summa duorum quadratorum inter se primorum $rr+ss$ habeat divisorem $4n+1$; consequenter cum hujusmodi summa duorum quadratorum alios non admittat divisores, nisi qui ipsi sint summae duorum quadratorum, necesse est, ut numerus primus $4n+1$ sit summa duorum quadratorum.

§ 29. **Coroll. 1.** Demonstratio haec igitur esset perfecta, si modo demonstrari posset, semper ejusmodi existere valores pro a et b substituendos, quibus formula $a^{2n}-b^{2n}$ non fiat divisibilis per numerum primum $4n+1$; iisdem enim casibus formula $a^{2n}+b^{2n}$ necessario est divisibilis per $4n+1$.

§ 30. **Coroll. 2.** Quod si quis autem hanc rem per calculum tentet, non modo semper plures casus, imo infinitos, formulae $a^{2n}-b^{2n}$ reperiet, quibus ea per numerum primum $4n+1$ non est divisibilis, sed etiam pro b unitatem ponere licet, ita, ut etiam haec formula simplicior $a^{2n}-1$ saepenumero per $4n+1$ non sit divisibilis.

§ 31. **Scholion.** Casus seu valores ipsius a, quibus formula $a^{2n}-1$ certe fit divisibilis per numerum primum $4n+1$, facile assignari possunt. Primo enim si sit $a=pp$, formula

$$a^{2n}-1=p^{4n}-1$$

semper est divisibilis per $4n+1$, dummodo p non sit $=4n+1$, vel ejus multiplo. Deinde si $a=pp\pm(4n+1)q$, formula $a^{2n}-1$ quoque divisorem habet $4n+1$; resolvitur enim

$$a^{2n}=(pp\pm(4n+1)q)^{2n}$$

in seriem terminorum, quorum primus est p^{4n}, sequentes vero omnes sponte sunt per $4n+1$ divisibiles. Unde patet, valores idoneos pro a esse omnia residua, quae restant, si numeri quadrati p^2 per $4n+1$ dividantur. Haec autem residua, sive pro a ponatur r, sive $4n+1+r$, sive $(4n+1)q+r$, prodeunt eadem, unde omnia possibilia residua obtinentur, si pro p successive statuantur numeri 1, 2, 3, 4, 5,... usque ad $4n$, at valor $4n$ pro p positus idem dat residuum, quod valor 1, similique modo valores 2 et $4n-1$, item 3 et $4n-2$, item 4 et $4n-3$ etc. eadem dant residua. Unde cum bina semper

residua quae ex numeris 1, 2, 3, ... usque ad $4n$ pro radicibus quadratorum sumtis proveniunt, sint aequalia, numerus diversorum residuorum resultantium tantum erit $2n$, ideoque totidem dabuntur numeri ipso $4n+1$ minores, qui non esse possunt residua ex divisione numerorum quadratorum per $4n+1$ emergentia; hique numeri pro a substituti semper formulam $a^{2n}-1$ reddent non divisibilem per $4n+1$. Hoc quidem pariter demonstrari nequit; verumtamen quia periculum faciendo, quotcunque etiam numeri hoc modo explorentur, ne unicus quidem casus occurret, quo haec regula fallat, ejus veritatem agnoscere oportet. Quo haec clarius perspiciantur, exempla aliquot subjungam: Sit primo $4n+1=5$, et casus, quibus formula a^2-1 per 5 erit divisibilis, habebuntur, si pro a residua ex divisione quadratorum per 5 oriunda ponantur, quae residua sunt 1, 4. At si pro a ponatur vel 2, vel 3, formula a^2-1 non erit per 5 divisibilis; his ergo casibus formula a^2+1 divisorem habebit 5. Deinde si sit $4n+1=13$, seu $n=3$, residua, quae ex divisione numerorum quadratorum per 13 restant, sunt 1, 4, 9, 3, 12, 10, unde si quis numerorum reliquorum, 2, 5, 6, 7, 8, 11, pro a substituatur, non formula a^6-1, sed a^6+1 per 13 erit divisibilis. Porro si $4n+1=17$, seu $n=4$, quia residua quadratorum per 17 divisorum sunt 1, 4, 9, 16, 8, 2, 15, 13, si pro a statuatur quispiam ex reliquis numeris 3, 5, 6, 7, 10, 11, 12, 14, non formula a^8-1, sed haec a^8+1 erit per 17 divisibilis. Cum igitur haec lex perpetuo observetur, haec inductio vim demonstrationis fere induere censenda erit; hincque propositio tantopere confirmata videtur, ut ejus veritatem non amplius in dubium vocare liceat. Interim tamen operae pretium esset eo majus, si quis rigorosam hujus propositionis demonstrationem exhibere posset, quo magis de ejus veritate sumus certi: nullum enim est dubium, quin ejusmodi demonstratio, tamdiu frustra quaesita, ad plurimas alias insignes numerorum proprietates sit manuductura. Quamquam autem hujus propositionis veritas extra dubium est posita, tamen eas consequentias, quae ipsi innituntur, diligenter notabo, ab aliisque, quae rigidis demonstrationibus muniuntur, distinguam: ex hac autem propositione nondum demonstrata sequuntur haec corollaria, quae hoc nomine notata velim.

§ 32. **Coroll. 3.** Si igitur numerus formae $4n+1$ in duo quadrata nullo modo resolvi nequeat, hoc certum erit signum, eum numerum non esse primum: si enim iste numerus $4n+1$ esset primus, certe in duo quadrata resolvi posset. Sic cum 21, 33, 57, 69, 77, 93, etc. qui in forma $4n+1$ continentur, non sint summae duorum quadratorum, ex hoc ipso patet, eos non esse primos.

§ 33. **Coroll. 4.** In serie ergo numerorum, qui sunt summae duorum quadratorum, omnes primo continentur numeri primi hujus formae $4n+1$, deinde omnia producta ex duobus pluribusve hujusmodi numeris primis; tam producta ex singulis hisce numeris in binarium et quosvis numeros quadratos.

§ 34. **Coroll. 5.** Omnes numeri n, ex quibus formula $4n+1$ evadit numerus primus, sunt summae duorum numerorum trigonalium. Cum enim $4n+1$ sit summa duorum quadratorum, erit ejus duplum $8n+2$ summa duorum quadratorum imparium: sit ergo

$$8n+2=(2x+1)^2+(2y+1)^2, \quad \text{fiet} \quad n=\frac{xx+x}{2}+\frac{yy+y}{2}.$$

Quare si n non sit summa duorum numerorum trigonalium, certe numerus $4n+1$ non erit primus.

§ 35. **Propositio VI.** *Si numerus formae* $4n+1$ *unico modo in duo quadrata inter se prima resolvi queat, tum certe est numerus primus.*

Demonstratio. Quoniam enim hic numerus est summa duorum quadratorum inter se primorum, si non sit primus, singuli ejus factores erunt summae duorum quadratorum. Quare si hic numerus non esset primus, in hujusmodi saltem duos factores resolvi posset, ut esset

$$4n+1=(aa+bb)(cc+dd);$$

hoc autem casu duplex resolutio in duo quadrata locum habet, scilicet:

$$\text{I.}\quad 4n+1=(ac+bd)^2+(ad-bc)^2,$$
$$\text{II.}\quad 4n+1=(ad+bc)^2+(ac-bd)^2.$$

Haeque resolutiones semper sunt diversae, nisi sit vel $ac+bd=ad+bc$, vel $ac+bd=ac-bd$. Priori vero casu foret $ac+bd-ad-bc=0$, seu $(a-b)(c-d)=0$, ideoque vel $a=b$, vel $c=d$; atque hinc vel $aa+bb$, vel $cc+dd$ numerus par, quorum neutrum esse potest divisor ipsius $4n+1$ utpote numeri imparis. Posteriori vero casu esset vel $b=0$, vel $d=0$, ideoque $4n+1$ vel $=aa(cc+dd)$, vel $=cc(aa+bb)$; unde haec duo quadrata non forent prima inter se, contra hypothesin. Quibus casibus notatis sequitur, numerum compositum $4n+1$, si in duo quadrata inter se prima fuerit resolubilis, eundem ad minimum duobus modis in duo quadrata esse resolubilem. Quocirca si tantum unico modo numerus $4n+1$ sit summa duorum quadratorum, certe non erit compositus, ac per consequens erit primus. Q. E. D.

§ 36. **Coroll. 1.** Si igitur proposito quopiam numero formae $4n+1$ post institutum examen comperiatur, eum unico modo in duo quadrata inter se prima resolvi posse, inde tuto colligemus, eum numerum esse primum; etiamsi ejus divisibilitatem per numeros primos more consueto non tentaverimus. Sic cum numerus 73 unico modo sit summa duorum quadratorum, nempe $64+9$, eum esse primum, certo novimus.

§ 37. **Coroll. 2.** Si ergo methodus expedita haberetur, cujus ope facile inquirere liceret, an et quot modis propositus numerus in forma $4n+1$ contentus in duo quadrata resolvi possit, exinde promte judicare poterimus, utrum sit primus; si enim unico modo in duo quadrata sit resolubilis, eaque quadrata fuerint prima inter se, is certe pro primo erit habendus.

§ 38. **Coroll. 3.** Manifestum autem est, si duo quadrata, in quae numerus quispiam resolvitur, non sint prima inter se, eum numerum non esse primum. Si enim numerus propositus inveniatur esse $=nnaa+nnbb$, tum divisores habebit n et nn: quod idem est intelligendum, si numerus propositus ipse sit quadratum, seu $=aa+0$, tum enim divisorem habebit a.

§ 39. **Scholion.** Haec regula numeros primos explorandi tantum ad numeros impares formae $4n+1$ est adstricta, numeri enim pares quandoque unico modo in duo quadrata resolvi possunt, cum tamen non sint primi; ita 10 unico modo est summa duorum quadratorum, etsi non est primus; cujus rei ratio est, quod in producto $(aa+bb)(cc+dd)$, cui hujusmodi numeri aequantur, est vel $a=b$, vel $c=d$, quo casu duplex resolutio, quae generatim innui videtur, ad unam redit, uti in demonstratione est animadversum. Neque vero hac exceptione regula data infringitur, cum numerorum parium per se facile sit judicium. Numeri autem impares alterius formae $4n-1$ hinc sponte excluduntur, quoniam ii plane non in duo quadrata sunt resolubiles. De cetero si numerus

$4n+1$ vel plane non resolubilis sit in duo quadrata, vel pluribus modis haec resolutio succedat, pro priori casu jam notavimus, eum numerum certe non esse primum, etsi hoc nititur propositione praecedente non satis rigide demonstrata. Pro casu vero posteriori in sequenti propositione judicium afferetur.

§ 40. **Propositio VII.** *Qui numerus duobus pluribusve diversis modis in duo quadrata resolvi potest, ille non est primus, sed ex duobus ad minimum factoribus compositus.*

Demonstratio. Sit numerus propositus N, qui duplici modo in duo quadrata sit resolubilis; nempe $N=aa+bb=cc+dd$. Quoniam haec quadrata non sunt aequalia, alioquin enim numerus N per se non esset primus, sit $a>b$ et $c>d$, et quia resolutiones hae duae sunt diversae, neque erit $a=c$, neque $b=d$. Sit igitur $a>c$; erit $b>d$: unde ponatur $a=c+x$ et $d=b+y$. Quare ob $aa+bb=cc+dd$, fiet: $2cx+xx=2by+yy$. Sit utraque forma $=xyz$, quia altera per x, altera per y est divisibilis; fiet $c=\frac{yz-x}{2}$; $b=\frac{xz-y}{2}$; $a=\frac{yz+x}{2}$; $d=\frac{xz+y}{2}$, hincque erit $N=aa+bb=\frac{xxzz+yy+yyzz+xx}{4}$, seu $N=\frac{(yy+xx)(1+zz)}{4}$. Nisi ergo $xx+yy$ per 4 sit divisibile, erit $xx+yy$ divisor ipsius N; sin autem $xx+yy$ sit per 4 divisibile, vel numerus utcunque compositus, ejus certe factor quidam erit divisor ipsius N. Cum igitur sit $x=a-c$ et $y=d-b$, numerus propositus $N=aa+bb=cc+dd$ divisorem habebit vel ipsum numerum $(a-c)^2+(d-b)^2$, vel ejus semissem quadrantemve, et quia numeros a, b et c, d, inter se utcunque permutare licet, factores ipsius N quoque erunt $(a-d)^2+(c-b)^2$, vel etiam quia radices a, b, c, d negative assumere licet $(a\pm c)^2+(d\pm b)^2$, vel $(a\pm d)^2+(c\pm b)^2$, seu harum formularum semisses aliaeve partes aliquotae. Quare cum numeri plus uno modo in duo quadrata resolubilis factores adeo assignari possint, ille numerus certe non erit primus, sed compositus. Q. E. D.

§ 41. **Coroll. 1.** Cum igitur numerus $N=aa+bb=cc+dd$ sit compositus, erit hujusmodi $N=(pp+qq)(rr+ss)$. Hinc autem vicissim duplex resolutio in duo quadrata resultat, erit nempe:

$$a=pr+qs \qquad \qquad c=ps+qr$$
$$\text{et}$$
$$b=ps-qr \qquad \qquad d=pr-qs.$$

Hincque ulterius obtinetur $a-d=2qs$ et $c-b=2qr$, unde fit $\frac{r}{s}=\frac{c-b}{a-d}$. Quare si fractio $\frac{c-b}{a-d}$ ad minimos terminos reducatur, ut sit $\frac{c-b}{a-d}=\frac{r}{s}$, ex hac fractione $\frac{r}{s}$ orietur numeri N divisor $=rr+ss$, nisi sit par; nam si fuerit par, ejus dimidium sumi debet.

§ 42. **Coroll. 2.** Simili modo cum numeros a, b et c, d inter se permutare atque adeo negativos ponere liceat, si fractionum harum $\frac{a\pm c}{b\pm d}$, vel $\frac{a\pm d}{b\pm c}$ altera ad minimos terminos reducatur, ut fiat $=\frac{r}{s}$, erit $rr+ss$ semper divisor numeri propositi N.

§ 43. **Coroll. 3.** Quanquam autem hinc plures duobus divisores nasci videntur, tamen diversae formulae ita ad eundem divisorem deducunt, ut non plures quam duo eliciantur, si quidem numerus propositus duobus tantum modis in duo quadrata fuerit resolubilis. Sic, si

$$N=85=9^2+2^2=7^2+6^2,$$

formulae $\frac{9\pm7}{6\pm2}$, $\frac{9\pm6}{7\pm2}$ has quatuor tantum fractiones in minimis terminis suppeditant nempe; $\frac{2}{1}$; $\frac{1}{2}$; $\frac{5}{3}$; $\frac{3}{5}$; quarum binae posteriores pro formula $rr+ss$ duplum valorem tantum exhibent ejus, qui ex primis oritur: unde patebit, factores esse binos $2^2+1=5$ et $4^2+1=17$. Brevissime ergo hi factores inveniuntur, si tamen radices quadratorum pares et impares seorsim invicem combinentur, et combinatio parium cum imparibus penitus omittatur, quia hinc fractiones orirentur, numeratorem et denominatorem impares habentes.

§ 44. **Problema.** *Proposito numero quocunque formae* $4n+1$, *explorare utrum primus sit nec ne?*

Solutio. Per operationem deinceps explicandam investigetur numerus propositus, utrum in duo quadrata resolvi posset nec ne? et, si possit, an plus uno modo resolutio succedat? Si enim resolutionem in duo quadrata plane non admittat, id per § 32 certum erit signum, numerum propositum non esse primum, etiamsi haec conclusio ex propositione quinta non satis demonstrata sequatur. Hoc quidem casu de ejus divisoribus nihil constat; interim tamen certo colligimus, eum divisores primos habere formae $4m-1$, quia si omnes ejus factores essent formae $4m+1$, is certe in duo quadrata foret resolubilis. At si numerus propositus unico modo sit in duo quadrata resolubilis, tum infallibiliter pro primo erit habendus. Sin autem resolutio plus uno modo succedat, tum non solum constabit, eum non esse primum, sed etiam ejus divisores assignari poterunt per § 43. His perpensis regulam tradam, cujus ope resolubilitas in duo quadrata non difficulter explorari poterit.

Numerus propositus desinet vel in 1, vel in 3, vel in 7, vel in 9; casum quo in 5 desinit hic omitto, quia divisor 5 tum est manifestus, et indicat numerum non esse primum. Deinde numeri quadrati, incipiendo a maximis ipso numero proposito minoribus, successive ab eo subtrahantur, ut pateat, utrum unquam numerus quadratus restet; quoties enim hoc evenit, toties resolutio in duo quadrata succedit.

At cum numeri quadrati in nullum horum numerorum 2, 3, 7, 8, desinere queant, subtractio eorum numerorum quadratorum, qui residua dant in hos numeros desinentia, omitti poterit. Hinc tantum opus est ut a numero proposito ea quadrata subtrahantur, quae residua in 0, 1, 4, 5, 6, 9, desinentia praebent; nempe

si numerus propositus desinat in	quadrata subtrahenda desinent in	et horum quadratorum radices desinent in
1	0, 1, 5, 6	0, 1, 4, 5, 6, 9
3	4, 9	2, 3, 7, 8
7	1, 6	1, 4, 6, 9
9	0, 4, 5, 9	0, 2, 3, 5, 7, 8.

Pro quolibet igitur numero proposito $4n+1=N$ tot operationes seorsim substituantur, quot radicum idoneae sunt terminationes. Sit igitur pp maximum quadratum hujus indolis, quod a numero proposito N subtrahi debet: ac tum successive subtrahantur quadrata $(p-10)^2$, $(p-20)^2$, $(p-30)^2$, $(p-40)^2$, etc. Verum residua hinc emergentia expedite per continuam additionem inveniri poterunt hoc modo:

$$\begin{array}{ll}
\text{Numerus propositus} \ldots\ldots\ldots\ldots & N \\
\quad\text{a quo subtrahatur} \ldots\ldots\ldots & pp \\
\hline
 & N - pp \\
\quad\text{addatur} \ldots\ldots\ldots\ldots\ldots & 20\,p - 100 \\
\hline
 & N - (p - 10)^2 \\
\quad\text{addatur} \ldots\ldots\ldots\ldots\ldots & 20\,p - 300 \\
\hline
 & N - (p - 20)^2 \\
\quad\text{addatur} \ldots\ldots\ldots\ldots\ldots & 20\,p - 500 \\
\hline
 & N - (p - 30)^2
\end{array}$$

Numeri igitur successive addendi sunt:

$$20p - 100,\ 20p - 300,\ 20p - 500,\ 20p - 700,\ \text{etc.}$$

qui decrescunt in ratione arithmetica per differerentiam $= 200$. Hujusmodi operatio pro singulis numeris p, quorum quadrata numero proposito proxime sunt minora, et qui desinunt in aliquem figurarum supra indicatarum, instituatur, neque ulterius continuetur, quam donec ad semissem numeri propositi N perveniatur. Si enim numerus N fuerit summa duorum quadratorum, alterum certe semissi ipsius minus sit necesse est. Quo observato, quot hac operatione prodibunt quadrata, tot modis numerus propositus in duo quadrata erit resolubilis. Hanc autem operationem non admodum esse molestam, omnibusque aliis methodis numeros primos explorandi longe anteferendam, sequentia exempla declarabunt.

§ 45. *Exempl. 1. Explorare utrum hic numerus* 82421 *primus sit nec ne?*

Operatio per sex columnas sequentes instituetur:

p 82421	p 82421	p 82421	p 82421	p 82421	p 82421
286. 81796	285. 81225	284. 80656	281. 78961	280. 78400	279. 77841
□ 625	1196	1765	3460	4021	4580
5620	5600	5580	5520	5500	5480
6245	6796	7345	8980	9521	10060
5420	5400	5380	5320	5300	5280
11665	12196	12725	14300	14821	15340
5220	5200	5180	5120	5100	5080
16885	17396	17905	19420	19921	20420
5020	5000	4980	4920	4900	4880
21905	22396	22885	24340	24821	25300
4820	4800	4780	4720	4700	4680
26725	27196	27665	29060	29521	29980
4620	4600	4580	4520	4500	4480
31345	31796	32245	33580	34021	34460
4420	4400	4380	4320	4300	4280
35765	36196	36625	37900	38321	38740
4220	4200	4180	4120	4100	4080
39985	40396	40805	42020	42421	42820

Cum igitur hic unicum occurrat quadratum 625, ideoque numerus propositus 82421 unico modo fit in duo quadrata resolubilis, nempe $= 25^2 + 286^2$, is erit primus.

§ 46. **Scholion.** In hoc computo quatuor columnae, ubi numeri residui desinunt vel in 5, vel in 0, notabiliter contrahi possunt, omittendis omnibus iis, qui non desinunt vel in 25, vel in 00. Quare in columnis, in quibus residua desinunt vel in 5, vel in 0, subtrahatur primo proximum quadratum, quod residuum praebet vel in 25, vel in 00 desinens, hocque quadratum dicatur pp, ut residuum sit $= N - pp$: tum quadrata, unde residua simili modo desinentia oriuntur, erunt $(p - 50)^2$, $(p - 100)^2$, $(p - 150)^2$ etc. ideoque haec residua obtinebuntur, si ad $N - pp$ continuo addantur hi numeri $100p - 2500$; $100p - 7500$; $100p - 12500$, qui decrescunt arithmetice secundum differentiam constantem 5000, unde hae columnae mox ad finem perducentur, dum eas non ultra semissem numeri propositi continuari opus est. Hoc igitur compendium locum habebit in numeris vel in 1, vel in 9 desinentibus, qui propterea, etiamsi sex columnas requirant, dum pro reliquis quatuor sufficiunt, facilius expedientur.

§ 47. *Exempl.* 2. *Explorare utrum hic numerus* 100981 *primus sit nec ne?*

p. 100981	*p.* 100981	*p.* 100981	*p.* 100981
316. 99856	315. 99225	309. 95481	310. 96100
1125	1756	5500	4881
29100	6200	28400	6100
30225	7956	33900	10981
24100	6000	23400	5900
* 54325	13956	* 57300	16881
	5800		5700
p 100981	19756	100981	22581
284. 80656	5600	291. 84681	5500
20325	25356	16300	28081
25900	5400	26600	5300
$215^2 = 46225$	30756	42900	33381
	5200	21600	5100
	35956	* 64500	38481
	5000		4900
	40956		43381
	4800		4700
	45756		48081
	4600		
	50356		

Cum ergo unicum occurrat quadratum $46225 = 215^2$, unde fit $100981 = 215^2 + 234^2$, erit hic numerus primus.

§ 48. *Exempl. 3. Explorare utrum hic numerus* **1000009** *sit primus nec ne?*

p 1000009		*p* 1000009	*p* 1000009	*p* 1000009	
1000. 1000000		978. 956484	997. 994009	995. 990025	
$3^2 = 9$	277509	43525	6000	9984	285984
19900	16900	95300	97200	19800	16800
19909	294409	138825	103200	29784	302784
19700	16700	90300	92200	19600	16600
39609	311109	229125	195400	49384	319384
19500	16500	85300	87200	19400	16400
59109	327609	314425	282600	68784	335784
19300	16300	80300	82200	19200	16200
78409	343909	394725	364800	87984	351984
19100	16100	75300	77200	19000	16000
97509	360009	470025	442000	106984	367984
18900	15900			18800	15800
116409	375909	*p* 1000009	*p* 1000009	125784	383784
18700	15700	972. 944784	953. 908209	18600	15600
135109	391609	$235^2 = 55225$	91800	144384	399384
18500	15500	94700	92800	18400	15400
153609	407109	149925	184600	162784	414784
18300	15300	89700	87800	18200	15200
171909	422409	239625	272400	180984	429984
18100	15100	84700	82800	18000	15000
190009	437509	324325	355200	198984	444984
17900	14900	79700	77800	17800	14800
207909	452409	404025	433000	216784	459784
17700	14700	74700		17600	14600
225609	467109	478725		234384	474384
17500	14500			17400	14400
243109	481609			251784	488784
17300	14300			17200	
260409	495909			268984	
17100				17000	
277509				285984	

Hic ergo numerus 1000009 duplici modo est in duo quadrata resolubilis, quippe

$$= 1000^2 + 3^2 = 235^2 + 972^2,$$

unde is non erit primus: factores vero ejus reperientur ex hac formula $\frac{1000 \pm 972}{235 \pm 3}$ ad minimos terminos reducta, unde oritur:

$$\frac{1000+972}{235+3} = \frac{1972}{238} \overset{2}{\Big|} \frac{986}{119} \overset{17}{\Big|} \frac{58}{7}, \text{ ergo factor } = 3413$$

$$\frac{1000+972}{235-3} = \frac{1972}{232} \overset{4}{\Big|} \frac{493}{58} \overset{29}{\Big|} \frac{17}{2}, \text{ ergo factor } = 293,$$

qui factores facilius invenientur ex formula

$$\frac{1000-972}{235\pm 3}=\frac{28}{238}=\frac{14}{119}=\frac{2}{17} \text{ et } \frac{28}{232}=\frac{7}{58}.$$

Novimus ergo esse $1000009 = 293.3413$, qui factores nulla alia methodo tam facile reperti fuissent.

§ 49. *Exempl.* 4. *Explorare utrum hic numerus* 233033 *primus sit nec ne?*

233033	233033	233033	233033
$482^2 = 232324$	$477^2 = 227529$	$473^2 = 223729$	$478^2 = 228484$
709	5504	9304	4549
9540	9440	9360	9460
10249	14944	18664	14009
9340	9240	9160	9260
19589	24184	27824	23269
9140	9040	8960	9060
28729	33224	36784	32329
8940	8840	8760	8860
37669	42064	45544	41189
8740	8640	8560	8660
46409	50704	54104	49849
8540	8440	8360	8460
54949	59144	62464	58309
8340	8240	8160	8260
63289	67384	70624	66569
8140	8040	7960	8060
71429	75427	78584	74629
7940	7840	7760	7860
79369	83264	86344	82489
7740	7640	7560	7660
87109	90904	93904	90149
7540	7440	7360	7460
94649	98344	101264	97609
7340	7240	7160	7260
101989	105584	108424	104869
7140	7040	6960	7060
109129	112624	115384	111929
6940	6840	6760	6860
116069	* 119464	* 122144	* 118789

Quia ergo hic numerus, etsi est formae $4n+1$, non est summa duorum quadratorum, vi propositionis quintae colligimus eum non esse numerum primum. Factores quidem ejus hinc assignare non licet, interim tamen concludimus eum saltem duos habere factores formae $4m-1$: qui, investigatione instituta, reperientur 467. 499.

§ 50. *Exempl.* 5. *Explorare utrum hic numerus* 262657 *primus sit nec ne?*

262657 $511^2 = 261121$	262657 $509^2 = 259081$	262657 $506^2 = 256036$	262657 $504^2 = 254016$
1536 10120	3576 10080	6621 10020	8641 9980
11656 9920	13656 9880	$129^2 =$ 16641 9820	18621 9780
21576 9720	23536 9680	26461 9620	28401 9580
31296 9520	33216 9480	36081 9420	37981 9380
40816 9320	42696 9280	45501 9220	47361 9180
50136 9120	51976 9080	54721 9020	56541 8980
59256 8920	61056 8880	63741 8820	65521 8780
68176 8720	69936 8680	72561 8620	74301 8580
76896 8520	78616 8480	81181 8420	82881 8380
85416 8320	87096 8280	89601 8220	91261 8180
93736 8120	95376 8080	97821 8020	99441 7980
101856 7920	103456 7880	105841 7820	107421 7780
109776 7720	111336 7680	113661 7620	115201 7580
117496 7520	119016 7480	121281 7420	122781 7380
125016 7320	126496 7280	128701 7220	130161 7180
* 132336	* 133776	* 135921	* 137341

Cum igitur hic unicum quadratum occurrat $16641 = 129^2$, ita ut sit unico modo

$$262657 = 129^2 + 496^2,$$

hique numeri 129 et 496 sint inter se primi, certum est numerum 262657 esse primum.

§ 51. ***Exempl.* 6.** *Explorare utrum hic numerus* **32129** *sit primus nec ne?*

32129	32129	32129	32129
$152^2 = 23104$	$177^2 = 31329$	$175^2 = 30625$	$170^2 = 28900$
$95^2 = 9025$	800	1504	3229
12700	15200	3400	3300
* 21725	16000	4904	6529
		3200	3100
32129	32129	8104	9629
$148^2 = 21904$	$173^2 = 29929$	3000	2900
10225	2200	11104	12529
12300	14800	2800	2700
* 22525	* 17000	13904	15229
		2600	2500
		* 16504	* 17729

Hic igitur numerus quoque unico modo est in duo quadrata resolubilis $= 95^2 + 152^2$, sed quia hi numeri 95 et 152 non sunt primi inter se, sed communem divisorem habent 19, numerus propositus non erit primus, sed factorem habet $19^2 = 361$, estque $32129 = 19^2 . 89$.

§ 52. **Scholion.** Quanquam haec methodus explorandi numeros utrum sint primi nec ne? tantum ad numeros in hac forma $4n + 1$ contentos extenditur, tamen saepenumero in dijudicandis numeris magnum subsidium afferre potest. Quantum autem aliis regulis hoc idem praestandi antecellat, quilibet, qui periculum hujus rei facere velit, facile experietur. Qui enim numerum millione non minorem via consueta examinare voluerit, ejus divisionem per omnes numeros primos ad millenarium usque tentare debet, quod opus intra plures horas non absolvet: dum ope hujus regulae ipsi vix semihora opus erit.



XIII.

Specimen de usu observationum in mathesi pura.

(N. Comment. VI. 1756 — 57. p. 185. Exhib. 1754. Sept. 30.)

Inter tot insignes numerorum proprietates, quae adhuc sunt inventae ac demonstratae, nullum est dubium, quin pleraeque primum ab inventoribus tantum sunt observatae et in multiplici numerorum tractatione animadversae, antequam de iis demonstrandis cogitaverint. Ita de eo numerorum primorum ordine, qui unitate superant multiplum quaternarii, cujusmodi sunt 5, 13, 17, 29, 37 41, etc. ante sine dubio est observatum, eorum singulos in duo quadrata secari posse, quam in eo elaboratum, ut hujus observationis veritas per solidam demonstrationem evinceretur. Quod deinde quilibet numerus in quatuor vel pauciora quadrata distribui possit, Diophanto jam notum fuisse videtur, nemo autem ante Fermatium est professus, se hujus veritatis demonstrationem habere, quam autem nusquam publice edidit, ita ut mea demonstratio, quam ante aliquod tempus concinnavi, pro prima, quae quidem publice fuerit proposita, sit habenda (*). Interim tamen fateri cogor, demonstrationem Fermatianam, etiamsi mihi nihil omnino de principiis, quibus innitebatur, suspicari licuerit, mea multo fuisse perfectiorem, ac longe latius patuisse. Asseverat enim Fermatius, se ex eodem fonte aliorum quoque theorematum demonstrationes hausisse, cujus generis sunt, quod omnis numerus integer sit summa trium pauciorumve numerorum trigonalium: item quod omnis numerus integer sit summa quinque vel pauciorum numerorum pentagonalium; item sex pauciorumve numerorum hexagonalium, et ita porro de reliquis numeris polygonalibus in infinitum. Ego vero etiamsi resolutionem cujusque numeri in quatuor pauciorave quadrata demonstravi, tamen omnem adhuc operam in istis reliquis theorematibus demonstrandis inutiliter consumsi, neque ullo modo etiam nunc saltem resolutionem in tres paucioresve trigonales ostendere potui, etiamsi ea simplicior videatur, quam resolutio in quatuor pauciorave quadrata. Verum et has eximias numerorum proprietates Fermatius multo ante per inductionem conclusisse est putandus, quam eas demonstrare didicerit. Ex quibus merito colligimus, in numerorum indole scrutanda observationi et inductioni, cui omnes has elegantissimas proprietates acceptas referre debemus, plurimum esse tribuendum; ideoque ne nunc quidem ab hoc negotio ulterius prosequendo esse desistendum. Hoc enim modo pertingimus ad hujusmodi proprietatum cognitionem, quae alias nobis perpetuo ignotae mansissent; ac tum demum occasionem nanciscimur ad investigationem demonstrationum vires nostras intendendi; veritates namque pleraeque hujus generis ita sunt comparatae, ut prius agnosci debeant, quam demonstrari possint. Quamvis autem hujusmodi proprietas per assiduam observationem fuerit animadversa, quae per se menti non parum est jucunda, tamen nisi demonstratio solida accesserit, de ejus veritate non satis certi esse possumus; exempla enim non desunt, quibus sola inductio in errorem praecipitaverit. Tum vero

(*) Vide Supplenda in fine tomi II hujus operis.

ipsa demonstratio non solum omnia dubia tollit, sed etiam naturae numerorum penetralia non mediocriter recludit, nostramque numerorum cognitionem continuo magis promovet, a cujus certe doctrinae perfectione adhuc longissime sumus remoti. Verum si cui haec forte non magni momenti esse videantur, quod vix unquam ullum in mathesi applicata usum habitura putentur, usus quem inde in ratiocinando adipiscimur, certe non est contemnendus. Sunt enim plerumque hujus generis veritates ita reconditae, ut earum demonstrationes tam incredibilem circumspectionem, quam eximiam ingenii vim requirant. Quare cum vulgo ad ratiocinii facultatem comparandam demonstrationes geometricae commendari soleant, quippe quae regularum ratiocinandi usum maxime contineant, nescio an non ad hunc scopum demonstrationes arithmeticae multo magis sint accommodatae: in his enim multo majori cura est cavendum, ne a praescriptis logicorum regulis aberremus, quoniam plerumque nimis est difficile, in errorem non prolabi. Deinde vero hujus generis demonstrationes arithmeticae multo majorem sollertiam et sagacitatem ingenii postulant, quam geometricae: unde qui in his fuerit exercitatus, longe facilius errorem in ratiocinando usu edoctus evitabit, sibique promtum ratiocinii usum multo certius comparabit. Atque, ob haec tam insignia commoda, perlustrationes naturae numerorum minime relinquendae videntur, in quibus ne inutiliter versemur, ab observationibus erit exordiendum, hincque ad demonstrationem proprietatum observatarum progrediendum. Hujusmodi operationem jam ante aliquot annos confeci in contemplatione divisorum cujusque numeri, qui est summa duorum quadratorum(*), nunc igitur, ut viam ad alias numerorum proprietates cognoscendas sternam, contemplaturus sum numeros, qui ex quadrato et duplo quadrati sunt compositi, quales in hac forma generali $2aa + bb$ sunt contenti, atque in divisores horum numerorum sum inquisiturus. At hic quidem statim notari convenit, radices horum duorum quadratorum numeros inter se primos esse oportere, alioquin enim quilibet numerus posset esse divisor, quadratum scilicet numeri, qui foret radicum communis divisor: quam ob rem numeros a et b, ex quibus forma $2aa + bb$ componitur, inter se primos statuam.

Consideratio circa numeros in hac forma $2aa + bb$ *contentos.*

Exponantur primo numeri in forma $2 + bb$ contenti, tum numeri hujus formae $8 + bb$, exclusis numeris paribus pro b substituendis: tertio numeri formae $18 + bb$, sumendo pro b numeros per 3 non divisibiles: quarto numeros formae $32 + bb$, sumendo pro b numeros per 2 non divisibiles, et ita porro. Sicque obtinebuntur sequentes numerorum progressiones:

$2 + bb$) 3, 6, 11, 18, 27, 38, 51, 66, 83, 102, 123, 146, 171, 198, 227, 258, 291, 326, 363, 402, 443, 486.

$8 + bb$) 9, 17, 33, 57, 89, 129, 177, 233, 297, 369, 449.

$18 + bb$) 19, 22, 34, 43, 67, 82, 118, 139, 187, 214, 274, 307, 379, 418.

$32 + bb$) 33, 41, 57, 81, 113, 153, 201, 257, 321, 393, 473.

$50 + bb$) 51, 54, 59, 66, 86, 99, 114, 131, 171, 194, 219, 246, 306, 339, 374, 411, 491.

$72 + bb$) 73, 97, 121, 193, 241, 361, 433.

$98 + bb$) 99, 102, 107, 114, 123, 134, 162, 179, 198, 219, 242, 267, 323, 354, 387, 422, 459, 498.

(*) Vide Comment. VI. pag. 35 seqq.

$128 + bb$) 129, 137, 153, 177, 209, 249, 297, 353, 417, 489.

$162 + bb$) 163, 166, 178, 187, 211, 226, 262, 283, 331, 358, 418, 451.

$200 + bb$) 201, 209, 249, 281, 321, 369, 489.

$242 + bb$) 243, 246, 251, 258, 267, 278, 291, 306, 323, 342, 386, 411, 438, 467, 498.

$288 + bb$) 289, 313, 337, 409, 457.

$338 + bb$) 339, 342, 347, 354, 363, 374, 387, 402, 419, 438, 459, 482.

$392 + bb$) 393, 401, 417, 473.

$450 + bb$) 451, 454, 466, 499.

Observatio. 1. Excerpamus hinc numeros primos, ut nanciscamur omnes numeros primos formae $2aa + bb$, qui quidem 500 non superent, quippe ad quem terminum omnes progressiones praecedentes produximus, atque isti numeri primi reperientur esse:

3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97, 107, 113, 131, 137, 139, 163, 179, 193, 211, 227, 233, 241, 251, 257, 280, 283, 307, 313, 331, 337, 347, 353, 379, 401, 409, 419, 433, 443, 449, 457, 467, 491, 499.

De his ergo observo, singulos nonnisi semel in serie numerorum formae $2aa + bb$ occurrere: *ita ut numerus primus, qui fuerit aggregatum ex quadrato et duplo quadrato, sit unico modo hujusmodi aggregatum.*

Observatio 2. Si ex numeris expositis excerpantur ii, qui sunt producta ex binario et numero primo, illi in ordinem digesti erunt:

6, 22, 34, 38, 82, 86, 118, 134, 146, 166, 178, 194, 214, 226, 262, 274, 278, 326, 358, 386, 422, 454, 466, 482.

Ubi alii numeri non occurrunt, nisi ipsi numeri primi formae $2aa + bb$ duplicati, ac singuli hi quidem numeri semel tantum reperiuntur.

Qui ergo numerus primus in forma 2aa + bb *fuerit contentus, ejus quoque duplum erit numerus formae* 2aa + bb, *idque unico modo.*

Ceterum cum a et b sint numeri inter se primi, ideoque alter eorum certo impar, manifestum est, nullos dari in forma $2aa + bb$ numeros per 4 divisibiles.

Observatio 3. Cum in numeris expositis alii sint impares, alii pares, et quidem impariter pares, observo porro: *Si quis numerus impar inter illos numeros reperiatur, tum quoque ejus duplum certo occurrere; ac vicissim quicunque numerus par in illis numeris occurrit, ejus quoque semissis ibidem certo reperietur.*

Observatio 4. Quodsi jam reliquos numeros non primos spectemus, singulosque in suos factores primos resolvemus, unicuique autem in parenthesi adscribamus, quot vicibus occurrat, sequentes nanciscemur:

3^2 (1); 3^3 (1); 3. 11 (2); 3. 17 (2); 3. 19 (2); 3^4 (1); 3^2. 11 (2); 11^2 (1); 3. 41 (2); 3. 43 (2); 3^2. 17 (2); 3^2. 19 (2); 3. 59 (2); 11. 17 (2); 3. 67 (2); 11. 19 (2); 3. 73 (2); 3^5 (1); 3. 83 (2); 3. 89 (2); 17^2 (1); 3. 97 (2); 3^3. 11 (2); 3. 107 (2); 17. 19 (2); 3. 113 (2); 19^2 (1); 3. 11^2 (2); 3^2. 41 (2); 3^2. 43 (2); 3. 131 (2); 3. 137 (2); 3. 139 (2); 11. 41 (2); 3^3. 17 (2); 11. 43 (2); 3. 163 (2).

Hic jam observo omnia producta ex numeris primis formae $2aa + bb$ per quamcunque combinationem nata occurrere: *ita ut productum ex quotcunque numeris formae* $2aa + bb$ *semper sit numerus in quadratum et duplum quadratum resolubilis:* ac plus quidem uno modo, si ex diversis factoribus fuerit conflatus.

Observatio 5. Imprimis autem hic animadverto, in his numeris compositis nullos alios factores primos occurrere, nisi qui ipsi sint formae $2aa + bb$; unde colligo per inductionem:

Omnes numeros formae $2aa + bb$, *si quidem* a *et* b *sint numeri inter se primi, nullos alios divisores admittere primos, nisi qui ipsi sint hujus formae* $2aa + bb$.

Binarium quidem vidimus inter divisores occurrere posse, verum cum $2aa + bb$ casu $b = 0$ et $a = 1$ binarium praebeat, etiam ipsum binarium in forma $2aa + bb$ complecti licet.

Observatio 6. Cum ergo omnis numerus formae $2aa + bb$, existentibus a et b primis inter se, alios divisores primos non admittat, nisi qui in serie numerorum in observatione prima exhibitorum contineantur, si ipsis quidem binarius adjungatur: circa istos numeros primos observo, intra illos nullos numeros sive hujus formae $8n - 1$, sive hujus $8n - 3$ reperiri.

De numeris ergo primis formae $8n - 1$ *et* $8n - 3$ *affirmare licet, eos non solum non esse numeros formae* $2aa + bb$, *sed etiam ne divisores quidem esse posse ullius numeri formae* $2aa + bb$, *siquidem* a *et* b *sint primi inter se.*

Observatio 7. Numeris ergo primis hujus geminae formae $8n - 1$ et $8n - 3$ exclusis, praeter binarium nulli alii relinquuntur numeri primi, qui sint divisores numerorum formae $2aa + bb$, nisi qui in alterutra harum formarum $8n + 1$, vel $8n + 3$ contineantur; quos duplicis generis numeros primos conspectui exposuisse juvabit:

$8n + 1$) 17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257, 281, 313, 337, 353, 401, 409, 433, 449, 457.

$8n + 3$) 3, 11, 19, 43, 59, 67, 83, 107, 131, 139, 163, 179, 211, 227, 251, 283, 307, 331, 347, 379, 419, 443, 467, 491, 499.

atque observo, hos numeros primos omnes inter numeros primos formae $2aa + bb$ ita occurrere, ut alii praeterea ibi non reperiantur.

Hinc ergo numeri hujus formae $2aa + bb$, *dummodo* a *et* b *sint inter se primi, praeter binarium nullos alios habent divisores primos, nisi qui sint vel hujus formae* $8n + 1$, *vel hujus* $8n + 3$.

Cum autem omnes numeri primi in his quatuor formis $8n \pm 1$ et $8n \pm 3$ contineantur, haec observatio cum praecedente convenit.

Observatio 8. At, quod notatu maxime est dignum, observo:

Omnem numerum primum tam hujus formae $8n + 1$, *quam hujus* $8n + 3$, *semper esse aggregatum ex quadrato et duplo quadrato: sive inter numeros primos formae* $2aa + bb$ *omnes plane numeros, sive hujus formae* $8n + 1$, *sive hujus* $8n + 3$ *occurrere, ac praeterea nullos alios.*

Nullus ergo assignari poterit numerus primus in harum formularum $8n + 1$ et $8n + 3$ alterutra contentus, qui non sit summa quadrati et dupli quadrati, et hoc quidem unico modo, si observatio prima huc trahatur.

Nota. Proprietatum, quas hic circa numeros formae $2aa + bb$ eorumque divisores observavimus, aliae ita sunt comparatae, ut earum veritas facile ostendi possit, aliae autem majorem demonstrationis apparatum requirunt, aliae vero denique profundissimae indaginis sunt judicandae, cum summa sollertia ad eas demonstrandas sit opus. Ad primum genus referendae sunt observationes prima, secunda, tertia, quarta et pars prior sextae; ad genus secundum autem pertinent observationes quinta, pars posterior sextae, et septima, quae eo redit. Profundissimae autem indaginis est observatio octava. Proprietates autem istae similes sunt iis, quas circa summas duorum quadratorum proposui; quarum veritatem cum feliciter eruerim, operam dabo, ut etiam has proprietates observatas simili modo demonstrationibus confirmem. Incipiam ergo ab observationibus facillimis.

1. **Theorema 1.** Si numerus N fuerit numerus formae $2aa + bb$, tum quoque ejus duplum $2N$ erit numerus ejusdem formae.

Demonstratio. Sit enim $N = 2mm + nn$, erit $2N = 4mm + 2nn$, ponatur $2m = k$, fietque $2N = kk + 2nn$, sicque $2N$ erit quoque numerus formae $2aa + bb$. Q. E. D.

2. **Coroll. 1.** Ac si N fuerit pluribus modis numerus formae $2aa + bb$, totidem quoque modis ejus duplum $2N$ erit numerus formae $2aa + bb$.

3. **Coroll. 2.** Constat ergo veritas observationis secundae, simulque ratio perspicitur, cur numerorum, qui inter numeros formae $2aa + bb$ supra expositos bis occurrunt, eorum quoque dupla ibidem bis reperiantur.

4. **Theorema 2.** Si numerus par $2N$ fuerit numerus formae $2aa + bb$, tum quoque ejus semissis N erit numerus ejusdem formae.

Demonstratio. Posito $2N = 2mm + nn$, quo $2mm + nn$ sit numerus par, quoniam pars $2mm$ jam est par, necesse est, ut altera pars nn sit quoque numerus par, ideoque et ejus radix n. Ponatur ergo $n = 2k$, fietque $2N = 2mm + 4kk$, unde per 2 dividendo oritur $N = mm + 2kk$, ita ut quoque semissis N sit in forma $2aa + bb$ contentus. Q. E. D.

5. **Coroll. 1.** Hinc etiam evidens est, si numerus propositus par $2N$ fuerit pluribus modis numerus formae $2aa + bb$, totidem quoque modis ejus semissem N fore numerum ejusdem formae.

6. **Coroll. 2.** Si ergo numerus N fuerit unico modo numerus formae $2aa + bb$, tum etiam ejus duplum $2N$ unico modo erit numerus formae $2aa + bb$; si enim pluribus modis esset hujus formae, totidem quoque modis ejus semissis N foret ejusdem formae contra hypothesin.

7. **Coroll. 3.** Hinc autem porro duplicando numeri $4N$, $8N$, $16N$ etc. omnes unico tantum modo in forma $2aa + bb$ continebuntur, siquidem numerus simplex N unico modo in ista forma reperiatur.

8. **Coroll. 4.** Quod vero hic de unico modo resolutionis in formam $2aa + bb$ est dictum, patet quoque ad duos pluresve modos. Ex qualibet enim resolutione numeri N in formam $2aa + bb$, sponte nascitur resolutio numeri, sive dupli, sive dimidii, sicque observationem tertiam demonstratam dedimus.

9. **Theorema 3.** Si habeantur duo numeri M et N formae $2aa + bb$, erit quoque eorum productum MN numerus ejusdem formae.

Demonstratio. Sit enim $M=2aa+bb$, et $N=2cc+dd$, erit eorum productum
$$MN=4aacc+2aadd+2ccbb+bbdd;$$
addatur $0=4acbd-4acbd$, et habebitur
$$MN=4aacc+4acbd+bbdd+2aadd-4acbd+2ccbb$$
quae expressio manifesto est aggregatum ex quadrato et duplo quadrato, scilicet:
$$MN=(2ac+bd)^2+2(ad-cb)^2,$$
vel quod eodem redit, si terminos $+4acbd$ et $-4acbd$ permutemus, ut sit
$$MN=4aacc-4acbd+bbdd+2aadd+4acbd+2ccbb$$
habebimus quoque alio modo $MN=(2ac-bd)^2+2(ad+cb)^2$. Quare si uterque numerus M et N fuerit formae $2aa+bb$, erit quoque productum numerus ejusdem formae. Q. E. D.

10. **Coroll. 1.** Ob geminas formulas inventas, productum MN erit duplici modo numerus formae $2aa+bb$. Si enim sit $M=2aa+bb$ et $N=2cc+dd$, ac ponatur productum $MN=2pp+qq$, erit
$$\text{vel} \quad p=ad-cb \quad \text{et} \quad q=2ac+bd,$$
$$\text{vel} \quad p=ad+cb \quad \text{et} \quad q=2ac-bd.$$

11. **Coroll. 2.** Si fuerit vel $ad-cb$, vel $2ac-bd$ numerus negativus, pro p et q eorum valores affirmativi assumi poterunt; ex formulis enim quadratis perinde elicere licuisset priori casu $p=cb-ad$, posteriori vero $q=bd-2ac$. Numeri igitur negativi hoc modo pro radicibus quadratorum oriundi calculum nihil turbant.

12. **Coroll. 3.** Productum ergo duorum numerorum formae $2aa+bb$ duplici modo in eandem formulam resolvi poterit, nisi forte utraque resolutio ad eandem recidat, quod autem non evenit, nisi fuerit vel $cb=0$ et $bd=0$, vel $ac=0$, hoc est $b=0$, vel $a=0$, vel $c=0$, vel etiam $d=0$, alterque propterea numerorum propositorum, vel quadratus, vel duplum quadrati.

13. **Coroll. 4.** Si ergo ambo numeri fuerint primi, eorum productum semper est duplici modo resolubile in formam $2aa+bb$, nisi alter fuerit $=1$, vel $=2$. Cum enim tantum excipiantur casus, quibus alter est quadratum, vel duplum quadratum, uterque autem ponatur primus, excipiuntur tantum casus, quibus alter est vel 1, vel 2.

14. **Coroll. 5.** Si ambo numeri M et N fuerint aequales, seu $N=M$, ut sit $c=a$ et $d=b$, erit quidem duplici modo quadratum $MM=2pp+qq$, scilicet vel $p=0$ et $q=2aa+bb$, vel $p=2ab$ et $q=2aa-bb$. Sed prior resolutio $MM=2.0^2+(2aa+bb)^2$, minus ad scopum pertinere est censenda, quia alterum quadratum est evanescens. Sin autem esset vel $a=0$, vel $b=0$, utraque resolutio adeo ad unum rediret.

15. **Coroll. 6.** Patet hinc etiam productum ex tribus numeris L, M, N formae $2aa+bb$ quadruplici modo in formam eandem resolvi posse. Sit enim:
$$L=2aa+bb; \quad M=2cc+dd; \quad N=2ee+ff$$
ac sit primo $LM=2pp+qq$, erit uti vidimus:
$$\text{vel} \quad p=ad-cb \quad \text{et} \quad q=2ac+bd,$$
$$\text{vel} \quad p=ad+cb \quad \text{et} \quad q=2ac-bd.$$
Tum ergo, si ponatur productum $LMN=2xx+yy$, erit quoque duplici modo

$$\text{vel} \quad x = pf - eq \quad \text{et} \quad y = 2ep + fq,$$
$$\text{vel} \quad x = pf + eq \quad \text{et} \quad y = 2ep - fq.$$

Hinc ergo pro p et q valoribus inventis substituendis, reperietur

I. vel $x = 2ace + bde + bcf - adf$ et $y = 2ade + 2acf - 2bce + bdf$,

II. vel $x = 2ace - bde - bcf - adf$ et $y = 2ade + 2acf + 2bce - bdf$,

III. vel $x = 2ace + bde - bcf + adf$ et $y = 2ade - 2acf - 2bce - bdf$,

IV. vel $x = 2ace - bde + bcf + adf$ et $y = 2ade - 2acf + 2bce + bdf$.

16. **Coroll. 7.** Simili modo colligitur, productum ex quatuor numeris formae $2aa + bb$ octo diversis modis in formam eandem resolvi posse; casus tamen sunt excipiendi, quibus inter numeros propositos reperiuntur vel aequales, vel simplicia quadrata, vel quadrata dupla; his enim casibus vidimus resolutiones, quae in genere sunt diversae, convenire.

17. **Scholion.** Quod autem ad istas resolutiones attinet, earum vis perfecte intelligi nequit, nisi demonstraverimus, numeros primos plus uno modo in hac forma $2aa + bb$ non contineri. Si enim numeri primi plurimis modis essent resolubiles, de numeris compositis nihil certi definiri posset, nisi quod adhuc pluribus modis hujusmodi resolutiones admittant. Cum igitur prima observatio nos docuerit, numeros primos, qui quidem in ordine numerorum formae $2aa + bb$ continentur, nonnisi semel ibidem occurrere, hanc ipsam veritatem demonstrare aggrediar.

18. **Theorema 4.** Qui numerus duplici modo in formam $2aa + bb$ resolvi potest, is non est primus.

Demonstratio. Sit numerus N duplici modo in hanc formam resolubilis, ac ponatur

$$N = 2aa + bb \quad \text{et} \quad N = 2cc + dd,$$

ut tam numeri a et c, quam b et d, sint diversi. Multiplicetur prior aequatio per cc, altera per aa, atque illa ab hac subtracta, relinquet:

$$(aa - cc) N = aadd - bbcc = (ad - bc)(ad + bc).$$

Quod si jam numerus N esset primus, is in alterutro factore $ad - bc$, vel $ad + bc$, contineretur, necesse est. Verum cum addendis nostris formulis sit $2N = 2aa + bb + 2cc + dd$, auferatur utrinque $2ad + 2bc$, unde habebitur:

$$2N - 2ad - 2bc = 2aa + bb + 2cc + dd - 2ad - 2bc;$$
$$\text{sive} \quad 2N - 2ad - 2bc = aa + (a-d)^2 + cc + (c-b)^2.$$

At postremum hoc membrum, utpote summa quatuor quadratorum, certo est nihilo majus, ita ut sit $2N - 2ad - 2bc > 0$: unde fit: $N > ad + bc$. Cum ergo N sit major, quam $ad + bc$, multoque magis quam $ad - bc$, numerus N in neutro factore $ad - bc$, vel $ad + bc$, tanquam pars continetur. Fieri ergo nequit, ut numerus N, qui duplici modo in formam $2aa + bb$ est resolubilis, sit primus. Q. E. D.

19. **Coroll. 1.** Si ergo N fuerit numerus primus, certe plus uno modo in formam $2aa + bb$ non est resolubilis, quoniam, si plus uno modo resolvi posset, non esset primus, sicque habetur demonstratio observationis primae.

20. **Coroll. 2.** Quicunque ergo numerus primus vel plane non ad formam $2aa + bb$ reduci potest, vel unico tantum modo. Cavendum autem, ne hinc vicissim concludatur, omnem numerum,

qui unico tantum modo sit resolubilis, esse primum; hujusmodi enim conclusio regulis ratiocinandi adversaretur.

21. **Coroll. 3.** Si fuerit idem numerus $N = 2aa + bb$, itemque $N = 2cc + dd$, erit hinc, ut vidimus, $(aa - cc) N = (ad - bc)(ad + bc)$, ideoque:

$$N = \frac{(ad - bc)(ad + bc)}{aa - cc}.$$

Numerator ergo hujus fractionis non solum per denominatorem erit divisibilis, sed reductione ad integrum facta, simul factores numeri N innotescent.

22. **Coroll. 4.** Hoc ergo casu numerus N non solum non erit primus, sed etiam ejus factores hinc facile colligentur. Sic cum numerus 267 bis inter numeros formae $2aa + bb$ occurrat, scilicet: $267 = 2.7^2 + 13^2$ et $267 = 2.11^2 + 5^2$, ob $a = 7$, $b = 13$, $c = 11$ et $d = 5$, habebimus:

$$267 = \frac{(35 - 143)(35 + 143)}{(7 - 11)(7 + 11)} = \frac{108.178}{4.18} \quad \text{hincque} \quad 267 = \frac{6.178}{4} = 3.89.$$

23. **Theorema 5.** **Si numerus formae $2aa + bb$ fuerit divisibilis per numerum primum ejusdem formae, tum etiam quotus erit numerus ejusdem formae.**

Demonstratio. Sit numerus propositus $N = 2aa + bb$, ejusque divisor $P = 2pp + qq$, qui cum sit primus, numeri p et q erunt primi inter se. Denotet Q quotum ex hac divisione oriundum, ita ut sit

$$Q = \frac{N}{P} = \frac{2aa + bb}{2pp + qq}.$$

Cum igitur numerus $N = 2aa + bb$ sit divisibilis per $P = 2pp + qq$; erit quoque

$$pp(2aa + bb) = 2aapp + bbpp$$

per P divisibile: at $aaP = 2aapp + aaqq$ etiam manifesto per P est divisibile, unde quoque differentia horum numerorum $aaqq - bbpp$, per numerum primum P divisibilis sit necesse est. Quia vero est $aaqq - bbpp = (aq - bp)(aq + bp)$, alter horum duorum factorum $aq \pm bp$, per numerum primum P certo erit divisibilis. Ponatur ergo $aq \pm bp = mP = 2mpp + mqq$ hincque reperitur:

$$q = \frac{2mpp \mp bp}{q} + mq = \frac{p(2mp \mp b)}{q} + mq.$$

Cum itaque $\frac{p(2mp \mp b)}{q}$ sit numerus integer, numeri autem p et q inter se primi, necesse est, ut $2mp \mp b$ sit per q divisibile. Ponatur ergo $2mp \mp b = \mp nq$, eritque

$$b = nq \mp 2mp, \quad \text{et} \quad a = mq \pm np.$$

Hinc autem fit:

$$N = 2aa + bb = \begin{cases} 2mmqq \mp 4mnpq + 2nnpp \\ + nnqq \pm 4mnpq + 4mmpp, \end{cases}$$

$$\text{sive} \qquad N = (2mm + nn)(2pp + qq).$$

Quodsi ergo hic numerus N dividatur per numerum primum $P = 2pp + qq$, per quem divisibilis esse ponebatur, quotus erit $Q = 2mm + nn$, ideoque numerus formae $2aa + bb$. Q. E. D.

24. **Hypothesis.** Quoniam in sequentibus frequentissime sermo erit de numeris formae $2aa + bb$, item de numeris primis ejusdem formae: deinde vero etiam de numeris tam primis,

quam compositis, qui in hanc formam $2aa + bb$ non sunt resolubiles; ne indolem horum numerorum describendo nimis fiam prolixus, compendii causa sequentibus signis utamur. Denotent ergo litterae initiales alphabeti majusculae: A, B, C, D, E, etc. perpetuo inposterum numeros formae $2aa + bb$, idque in genere, sive sint primi, sive compositi; eaedem vero litterae commate notatae: A', B', C', D', E', etc. numeros in hac forma non contentos, sive primos, sive compositos. Deinde vero litterae initiales alphabeti germanici majusculae $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, $\mathfrak{E}$, etc. significent numeros tantum primos formae $2aa + bb$, qui sunt, ut supra vidimus, 3, 11, 17, 19, 41, 43, 59, 67, 73, etc., quibus binarius adjungi potest. Eaedem vero litterae commate notatae $\mathfrak{A}'$, $\mathfrak{B}'$, $\mathfrak{C}'$, $\mathfrak{D}'$, $\mathfrak{E}'$, etc. denotent numeros primos in forma $2aa + bb$ non contentos, qui ergo sunt: 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71, etc.

25. **Coroll. 1.** Hac ergo notatione recepta, in theoremate antecedente demonstratum est, si numerus A fuerit divisibilis per numerum $\mathfrak{A}$, quotum certo fore numerum B: vel si numerus A unum factorem habeat $\mathfrak{A}$, alterum factorem fore B, scilicet numerum formae $2aa + bb$. Vel etiam si $\frac{A}{\mathfrak{A}}$ fuerit numerus integer, erit is $= B$.

26. **Coroll. 2.** Si ergo numerus A per numerum quempiam P divisus producat quotum B', hoc est numerum in forma $2aa + bb$ non contentum, tum divisor ille P certe non erit $\mathfrak{A}$, seu non erit numerus primus formae $2aa + bb$. Erit ergo vel compositus ejusdem formae, vel plane non istius formae $2aa + bb$.

27. **Coroll. 3.** Secundum hunc autem notandi modum in theorematibus praecedentibus demonstravimus:

In primo scilicet esse $2A = B$,

in secundo vero esse $\frac{A}{2} = B$,

in tertio esse $AB = C$,

in quarto si fuerit $A = B$, seu si idem numerus duplici modo in forma $2aa + bb$ contineatur, tum non esse $A = \mathfrak{A}$.

28. **Theorema 6.** Si numerus formae $2aa + bb$ divisibilis fuerit per numerum, qui ista forma non contineatur, tum quotus neque erit numerus primus formae $2aa + bb$, neque productum ex meris hujusmodi numeris primis conflatum.

Demonstratio. Demonstrari ergo debet si numerus A divisibilis fuerit per numerum B', tum quotum neque fore $= \mathfrak{A}$, neque productum hujusmodi $\mathfrak{ABCD}$ etc. Si enim quotus esset $\mathfrak{A}$, seu $\frac{A}{B'} = \mathfrak{A}$, foret $\frac{A}{\mathfrak{A}} = B'$, quod per theorema praecedens fieri nequit. Sin autem quotus esset productum ex quotcunque numeris primis formae $2aa + bb$, scilicet $= \mathfrak{ABCD}$, ut esset $\frac{A}{B'} = \mathfrak{ABCD}$, foret utique $A = \mathfrak{ABCD}B'$, ideoque $\frac{A}{\mathfrak{A}} = \mathfrak{BCD}B'$. At est $\frac{A}{\mathfrak{A}} = B$, unde foret $B = \mathfrak{BCD}B'$, hincque $\frac{B}{\mathfrak{B}} = \mathfrak{CD}B'$: verum simili modo est $\frac{B}{\mathfrak{B}} = C$, ideoque $\frac{C}{\mathfrak{C}} = \mathfrak{D}B'$: at est $\frac{C}{\mathfrak{C}} = D$, et $\frac{D}{\mathfrak{D}} = E$, foret ergo tandem $E = B'$, quod esset absurdum: unde sequitur, quotum neque fore numerum primum formae $2aa + bb$, neque productum ex meris hujusmodi numeris primis constans. Q. E. D.

29. **Coroll. 1.** Cum igitur quotus neque sit numerus primus formae $2aa + bb$, neque ex meris numeris primis hujus formae conflatus, factores habebit, vel saltem unum factorem primum in forma $2aa + bb$ non contentum, seu litera $\mathfrak{A}'$ designandum.

30. **Coroll, 2.** Quoniam ergo factores quoti sunt quoque factores dividendi, perspicuum est, si numerus formae $2aa + bb$ divisorem habeat B', seu in forma $2aa + bb$ non contentum, tum eundem numerum insuper alium ad minimum habiturum esse divisorem primum, in forma $2aa + bb$ non contentum, seu si numerus A divisorem habeat B', tum certe etiam divisorem habebit alium $\mathfrak{B}'$.

31. **Coroll. 3.** Quod hic in genere de divisoribus formae A' ostensum est, valet etiam de divisoribus formae $\mathfrak{A}'$. Hinc si numerus formae $2aa + bb$ divisibilis fuerit per numerum primum in eadem forma non contentum, tum etiam quotus est divisibilis per numerum primum in eadem forma non contentum.

32. **Theorema 7.** Si numerus formae $2aa + bb$, quantumvis magnus, divisorem habuerit numerum P, neque tamen radices a et b ipsae per P sint divisibiles, tum alius numerus ejusdem formae exhiberi potest minor, quam $\frac{3}{4}PP$, qui per eundem divisorem P sit divisibilis.

Demonstratio. Posito numero $2aa + bb$ divisibili per P, quantumvis magnae fuerint radices a et b, eae semper ita exprimi possunt:

$$a = mP \pm c \quad \text{et} \quad b = nP \pm d$$

ut numeri c et d semissem ipsius P non excedant, neuterque evanescet, cum neque a, neque b per P sit divisibile. Sit ergo $c < \frac{1}{2}P$ et $d < \frac{1}{2}P$; atque his valoribus substitutis forma $2aa + bb$ abibit in sequentem:

$$(2mm + nn)\,PP \pm 4mcP \pm 2ndP + cc + 2dd,$$

quae cum sit divisibilis per P, necesse est, ut quoque ejus pars $2cc + dd$ per P sit divisibilis; quae est et numerus formae $2aa + bb$, et minor quam $\frac{3}{4}PP$. Dato ergo numero formae $2aa + bb$ divisibili per numerum quemcunque P, semper exhiberi poterit numerus minor, quam $\frac{3}{4}PP$, et ejusdem formae, qui per eundem numerum P futurus sit divisibilis. Q. E. D.

33. **Coroll. 1.** Existente ergo P divisore cujuspiam numeri A, dabitur numerus $B < \frac{3}{4}PP$ per P divisibilis, et quotus inde oriundus propterea erit minor quam $\frac{3}{4}P$: qui cum etiam sit divisor numeri B, si P sit divisor cujuspiam numeri formae $2aa + bb$, hinc innotescit quoque numerus alius minor quam $\frac{3}{4}P$, qui pariter erit divisor cujusdam numeri formae $2aa + bb$.

34. **Coroll. 2.** Proposito porro numero quocunque P, si inter numeros formae $2aa + bb$, minores quam $\frac{3}{4}PP$, nullus datur per P divisibilis, tum etiam plane nullus existet numerus formae $2aa + bb$ per P divisibilis.

35. **Theorema 8.** Si numerus primus in forma $2aa + bb$ non contentus, fuerit divisor cujusquam numeri hujus formae, neque radices seorsim per eum sint divisibiles, tum alius quoque numerus primus, priore minor, et in hac forma non contentus, exhiberi poterit, qui etiam futurus sit divisor cujuspiam numeri ejusdem formae, neque tamen singulae radices per eum sint divisibiles.

Demonstratio. Demonstrandum ergo est, si fuerit numerus primus $\mathfrak{A}'$ divisor cujuspiam numeri $A = 2aa + bb$, ita ut neque a, neque b per $\mathfrak{A}'$ sit divisibile, tum quoque dari alium numerum primum $\mathfrak{B}' < \mathfrak{A}'$, qui quoque futurus sit divisor numeri cujuspiam $B = 2cc + dd$, ita ut neque c, neque d per illum sit divisibile. Demonstravimus autem, exhiberi posse numerum $A < \frac{3}{4}\mathfrak{A}'\mathfrak{A}'$; unde si ponatur quotus $\frac{A}{\mathfrak{A}'} = Q$, erit $Q < \frac{3}{4}\mathfrak{A}'$, ideoque multo magis $Q < \mathfrak{A}'$. At per § 31 vel hic ipse quotus Q erit numerus primus $\mathfrak{B}'$, vel saltem divisorem habebit primum formae $\mathfrak{B}'$. Sit igitur vel ipse quotus Q, vel ejus divisor $= \mathfrak{B}'$, qui certe multo minor erit quam $\mathfrak{A}'$. Quare cum quotus Q sit divisor numeri A, etiam $\mathfrak{B}'$ erit ejus divisor. Manifestum autem est, hunc quotum ejusve divisorem $\mathfrak{B}'$ unitatem esse non posse, cum unitas non solum sit in forma $2aa + bb$ contenta, sed etiam in demonstratione theorematis 6 excludatur. Q. E. D.

36. **Coroll. 1.** Si ergo numeri cujuspiam $A = 2aa + bb$ divisor esset numerus primus $\mathfrak{A}'$ in ista forma non contentus, neque a et b per eum seorsim fuerit divisibile, tum alius quoque numerus primus illo minor $\mathfrak{B}'$ existeret divisor numeri cujuspiam $B = 2cc + dd$.

37. **Coroll. 2.** Cum autem A ita capi possit, ut sit $A < \frac{3}{4}\mathfrak{A}'\mathfrak{A}'$, ita etiam pro altero numero $\mathfrak{B}'$ inveniri poterit numerus $B < \frac{3}{4}\mathfrak{B}'\mathfrak{B}'$ per ea, quae in theoremate 7 sunt demonstrata.

38. **Coroll. 3.** Si numerus $A = 2aa + bb$ fuerit divisibilis per numerum primum $\mathfrak{A}'$, neque a et b per eum sint divisibiles, numeri a et b pro primis inter se assumi poterunt: si enim haberent communem factorem, eo sublato nihilominus praeberent numerum $2aa + bb$ per $\mathfrak{A}'$ divisibilem.

39. **Coroll. 4.** At si numerus $A = 2aa + bb$, existentibus a et b inter se primis, divisorem habeat $\mathfrak{A}'$, tum etiam numerus $B = 2cc + dd$ minor quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$ exhiberi poterit per $\mathfrak{A}'$ divisibilis, ita ut c et d sint inter se primi. Posito enim $a = m\mathfrak{A}' \pm c$ et $b = n\mathfrak{A}' \pm d$ (32), numeri c et d certe non erunt per $\mathfrak{A}'$ divisibiles, ac si quem alium habeant communem factorem, puta $c = kp$ et $d = kq$, etiam $2pp + qq$ per $\mathfrak{A}'$ erit divisibilis, existentibus p et q inter se primis: hocque casu multo magis $2pp + qq$ minus erit quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$.

40. **Coroll. 5.** Cum igitur existente $A = 2aa + bb$ divisibili per $\mathfrak{A}'$, et radicibus a et b inter se primis, exhiberi possit numerus $B = 2cc + dd$ minor quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$, ita ut c et d sint numeri inter se primi, qui sit quoque per $\mathfrak{A}'$ divisibilis, erit, ut vidimus, hic idem numerus B quoque per alium numerum primum $\mathfrak{B}' < \frac{3}{4}\mathfrak{A}'$ divisibilis.

41. **Coroll. 6.** Atque cum $B = 2cc + dd$, existentibus c et d numeris inter se primis, jam sit divisibilis per numerum primum $\mathfrak{B}'$ minorem quam $\mathfrak{A}'$, inde novus numerus $C = 2ee + ff$ per $\mathfrak{B}'$ quoque divisibilis inveniri poterit, ita ut e et f sint numeri primi inter se, et ipse numerus C minor quam $\frac{3}{4}\mathfrak{B}'\mathfrak{B}'$.

42. **Theorema 9.** Nullus datur numerus formae $2aa + bb$, existentibus a et b numeris inter se primis, qui divisibilis sit per ullum numerum primum in ista forma non contentum.

Demonstratio. Fingamus enim, per numerum primum $\mathfrak{A}'$ divisibilem esse numerum $A = 2aa + bb$, atque a et b esse numeros inter se primos: hicque numerus A, si non minor fuerit quam $\frac{3}{4}\mathfrak{A}'\mathfrak{A}'$, in minorem transformari poterit. Habebit autem tum hic numerus A alium

divisorem primum in forma $2aa + bb$ non contentum, qui sit $= \mathfrak{B}'$, eritque $\mathfrak{B}' < \frac{3}{4}\mathfrak{A}'$; at si fuerit $A > \frac{3}{4}\mathfrak{B}'\mathfrak{B}'$, reperietur novus numerus $B = 2cc + dd$ divisibilis per $\mathfrak{B}'$, ita ut c et d sint numeri inter se primi et $B < \frac{3}{4}\mathfrak{B}'\mathfrak{B}'$. Jam simili modo, cum b habeat divisorem $\mathfrak{B}'$, alium praeterea habebit divisorem ejusdem indolis $\mathfrak{C}' < \frac{3}{4}\mathfrak{B}'$, hincque porro novus numerus $C = 2ee + ff$ per $\mathfrak{C}'$ divisibilis reperietur, ut sit $C < \frac{3}{4}\mathfrak{C}'\mathfrak{C}'$, et e et f numeri primi inter se. Hoc modo procedendo continuo minores numeri formae $2aa + bb$ obtinerentur, qui divisibiles essent per numeros in forma $2aa + bb$ non contentos. Quare cum in minoribus numeris formae $2aa + bb$, siquidem a et b sint primi inter se, nullus occurrat, qui habeat divisorem in forma ista non contentum, ne in maximis quidem hujusmodi numeri existunt, atque idcirco nullus plane datur numerus formae $2aa + bb$, qui sit divisibilis per ullum numerum in ea forma non contentum, siquidem a et b sint primi inter se.

43. **Coroll. 1.** Jam ergo evicta est veritas observationis quintae, qua animadvertimus, numerum quemcunque formae $2aa + bb$, siquidem a et b sint numeri primi inter se, nullos alios habere divisores primos, nisi qui sint ejusdem formae.

44. **Coroll. 2.** Omnis ergo numerus formae $2aa + bb$, siquidem a et b sint primi inter se, vel ipse est primus, vel est productum ex duobus pluribusve numeris primis, qui omnes in forma $2aa + bb$ contineantur. Hujusmodi itaque numerus nullos alios admittit divisores, nisi qui sint ejusdem formae $2aa + bb$.

45. **Coroll. 3.** Nullus ergo numerus primus in forma $2aa + bb$ non contentus, cujusmodi sunt 5, 7, 13, 23, 29, 31, 37, 47, 53, etc. unquam divisor, vel factor esse poterit ullius numeri formae $2aa + bb$, siquidem a et b sint numeri primi inter se. Neque vero hac restrictione, quod numeri a et b inter se primi esse debeant, est opus, dummodo uterque non sit per illum numerum primum divisibilis. Si enim a et b communem habeant divisorem n, per illum numerum primum non divisibilem, ut sit $a = nc$ et $b = nd$, tum quia $2cc + dd$ non est divisibilis, neque etiam $nn(2cc + dd)$, seu $2aa + bb$, per illum erit divisibilis.

46. **Scholion.** Notetur probe vis hujus demonstrationis, quae omnino est singularis, et in hoc consistit, quod in minoribus numeris nullus reperiatur numerus formae $2aa + bb$, existentibus a et b numeris inter se primis, qui sit divisibilis per ullum numerum primum in ista forma $2mm + nn$ non contentum. Hinc enim conclusi, etiam ne in majoribus et maximis quidem numeris nullos dari per ejusmodi numeros primos divisibiles. Demonstravi enim, si in maximis tales darentur numeri, tum etiam inter minores, ac tandem minimos, futuros esse numeros ejusdem indolis. Neque vero opus est ad hanc demonstrationem nosse, in numeris minimis nullos dari numeros formae $2aa + bb$, per numerum primum, qui non sit ejusdem formae, divisibiles; hoc enim ipsum jam per se est absurdum, minores continuo exhiberi posse numeros formae $2aa + bb$, qui per numerum primum non ejusdem formae essent divisibiles. Namque tandem necessario perveniri oporteret ad numeros primos, qui cum sint formae $2aa + bb$, certe per nullum numerum primum a se diversum dividi possent. Quare si de quacunque alia forma $maa + bb$, existentibus a et b numeris inter se primis, demonstrari posset, quod si majores numeri ejus formae dentur per numerum primum non ejusdem formae divisibiles, tum etiam necessario minores dari numeros, qui quoque per numerum primum non ejusdem formae futuri sint divisibiles, tum tuto concludere possemus, nullos plane dari

numeros formae $maa + bb$, qui per ullum numerum primum in eadem forma non contentum sint divisibiles. Verum ut similis demonstratio locum habere possit, necesse est, ut $\frac{m+1}{4}$ non sit majus quam 1, alias enim theoremata 7 et 8 applicari non possent: unde hujusmodi demonstratio non valebit, nisi in formis $aa + bb$, $2aa + bb$ et $3aa + bb$. At in hac postrema quidem forma exceptionem facit divisor 2 in forma $3aa + bb$ non contentus; hoc enim casu fit $a = 1$ et $b = 1$, seu $3.1 + 1$ est forma simplicissima per 2 divisibilis, quae cum non sit minor quam 2^2, quotus quoque non minor prodit quam 2, ideoque hinc conclusio ad numerum primum minorem in forma $3aa + bb$ non contentum, non succedit.

47. **Theorema 10.** Si numerus formae $2aa + bb$ unico modo in hanc formam fuerit resolubilis, atque a et b fuerint primi inter se, tum ille numerus certo est primus.

Demonstratio. Si enim non esset primus, duos pluresve haberet factores primos formae $2aa + bb$, ideoque duobus pluribusve modis in formam $2aa + bb$ esset resolubilis, ut in theoremate 3 demonstravimus: pluralitas enim resolutionum in dubium vocari nequit, si factores illi, quos habent, fuerint inaequales. Verum etiamsi factores fuerint aequales, tamen resolutio plus uno modo succedit: nam si numerus propositus N sit $= (2aa + bb)^2$, erit

$$\text{I.} \quad N = 2.0^2 + (2aa + bb)^2$$

$$\text{et} \quad \text{II.} \quad N = 2(2ab)^2 + (2aa - bb)^2;$$

at si sit $N = (2aa + bb)^3$, erit

$$\text{I.} \quad N = 2(2a^3 + abb)^2 + (2aab + b^3)^2,$$

$$\text{II.} \quad N = 2(2a^3 - 3abb)^2 + (6aab - b^3)^2.$$

Porro si sit $N = (2aa + bb)^4$, erit quoque:

$$\text{I.} \quad N = 2.0^2 + (4a^4 + 4aabb + b^4)^2,$$

$$\text{II.} \quad N = 2(4a^3b + 2ab^3)^2 + (4a^4 - b^4)^2,$$

$$\text{III.} \quad N = 2(8a^3b - 4ab^3)^2 + (4a^4 - 12aabb + b^4)^2.$$

Ergo pluralitas resolutionum etiam locum habet, si factores fuerint aequales, dummodo resolutiones, quibus vel altera radix evanescit, vel ambae communem habeant divisorem, non excludantur. Hinc ergo patet, si numerus $2aa + bb$, existentibus a et b numeris primis inter se, unico modo fuerit resolubilis in hanc formam, tum eum certo esse primum. Q. E. D.

48. **Coroll. 1.** Proposito ergo numero quocunque, quem constat esse in forma $2aa + bb$ contentum, facile erit explorare, utrum sit primus, nec ne? Considerentur enim numeri a et b, qui si non fuerint primi inter se, statim habetur factor, sin autem sint primi, tum inde successive omnia quadrata duplicata $2aa$ subtrahentur, et dispiciatur, an usquam quadratum bb relinquatur, quod si praeter casum cognitum non eveniat, certo pronunciare poterimus, numerum propositum esse primum.

49. **Coroll. 2.** Sin autem numerus propositus plus uno modo in quadratum et duplum quadratum fuerit resolubilis, tum non solum novimus eum non esse primum, sed etiam ejus factores assignare poterimus, secundum ea, quae § 21 sunt tradita. Hic autem modus numeros examinandi satis expedite perfici potest, perinde atque ego jam ex natura summae duorum quadratorum similem modum exposui.

50. **Theorema 11.** Nullus numerus, qui vel in hac forma $8n-1$, vel in hac $8n-3$ continetur, dividere potest ullum numerum formae $2aa+bb$, siquidem a et b sint numeri primi inter se.

Demonstratio. Demonstrasse sufficiet, nullum numerum, vel formae $8n-1$, vel $8n-3$, unquam esse posse formae $2aa+bb$; cum enim haec forma $2aa+bb$ nullos alios admittat divisores, nisi qui in hac ipsa forma sint contenti, statim ac demonstraverimus, nullum numerum, vel formae $8n-1$, vel $8n-3$, in forma $2aa+bb$ contineri, simul certum erit, ne quidem divisorem hujus formae esse posse. Cum autem $8n-1$ et $8n-3$ sint numeri impares, videamus, quibus casibus forma $2aa+bb$ numeros impares producat: manifestum autem est, hoc fieri non posse, nisi b sit numerus impar; quo casu bb fiet numerus formae $8m+1$. Tum vero numerus a vel erit par, vel impar; priori casu erit aa formae $4n$, ideoque $2aa$ formae $8n$, unde expressio $2aa+bb$ abibit in numerum formae $8m+8n+1$, seu $8n+1$. Posteriori casu, quo a est numerus impar, erit aa numerus formae $4n+1$, ideoque $2aa$ formae $8n+2$, unde expressio $2aa+bb$ praebet hoc casu numerum formae $8m+1+8n+2$, seu formae $8n+3$. Forma ergo $2aa+bb$ alios numeros impares non continet, nisi qui fuerint vel formae $8n+1$, vel formae $8n+3$. Quare nullus numerus impar, vel formae $8n-1$, vel formae $8n-3$, unquam in forma $2aa+bb$ continetur, nec propterea ullius numeri $2aa+bb$ divisor existere potest, si quidem a et b sint numeri primi inter se. Q. E. D.

51. **Coroll. 1.** Si ergo a et b fuerint numeri primi inter se, numerus $2aa+bb$ nunquam erit divisibilis, vel per 5, vel per 7, vel per ullum numerum hujus seriei 5, 7, 13, 23, 29, 31, 37, 47, 53, 61, 71, 79, etc. neque etiam per ullum numerum non primum, vel in forma $8n-1$, vel in forma $8n-3$ contentum, quales sunt 15, 21, 39, 45, 55, 63, 69, 77, 85, 87, 93, 95, etc.

52. **Coroll. 2.** Omnes ergo numeri impares, qui unquam esse possunt divisores numerorum formae $2aa+bb$, siquidem a et b sint inter se primi, vel in hac formula $8n+1$, vel hac $8n+3$, continentur. Neque tamen ulli numeri compositi harum formularum, qui factores habent formae $8n-1$, vel $8n-3$, divisores numeri $2aa+bb$ existere possunt.

53. **Coroll. 3.** Etiamsi ergo producta

$$(8m-1)(8n-1), \quad (8m-1)(8n-3) \quad \text{et} \quad (8m-3)(8n-3)$$

in formis $8m+1$, vel $8m+3$ contineantur, tamen ea nunquam divisores ullius numeri formae $2aa+bb$ existere possunt, si quidem a et b fuerint numeri primi inter se.

54. **Coroll. 4.** Quoties ergo forma $2aa+bb$ fit numerus primus, is semper vel in hac numerorum serie $8n+1$, vel hac $8n+3$, continebitur, unde in his duabus seriebus etiam omnes divisores primi, vel saltem impares numerorum in formula $2aa+bb$ contentorum, reperientur.

55. **Scholion 1.** Utrum autem omnes numeri primi, qui in seriebus numerorum $8n+1$ et $8n+3$ occurrunt, vicissim sunt numeri formae $2aa+bb$, quaestio est altioris indaginis. Quousque quidem supra numeros primos formae $2aa+bb$ continuavimus, vidimus in illis omnes plane numeros primos, tam hujus formae $8n+1$, quam hujus $8n+3$, occurrere, unde omnes quoque numeri primi, in his duabus formulis contenti, simul in forma $2aa+bb$ contineri videntur: verum hujus veritatis demonstratio maxime est abstrusa. Viam tamen ad eam jam non parum praeparavimus, dum demonstravimus, omnes divisores formae $2aa+bb$ simul esse numeros ejusdem formae, siquidem a et b fuerint inter se primi: nam proposito numero primo quocunque P, sive formae $8n+1$, sive $8n+3$, si demonstrare potuerimus, dari quempiam numerum $2aa+bb$ per illum divisibilem, ita ut neque a, neque b per eum sit divisibile; simul erit certum, numerum P esse in forma $2mm+nn$ contentum.

56. **Scholion 2.** Quod autem omnis numerus primus in alterutra harum formularum $8n+1$ et $8n+3$ contentus necessario sit aggregatum ex quadrato et duplo quadrato, uti id in numeris minoribus, 500 non superantibus, evenire vidimus, equidem me nondum demonstrare posse fateor: haecque demonstratio multo magis ardua videtur, quam ea, qua probavi, omnem numerum primum formae $4n+1$ esse summam duorum quadratorum. Cum autem momentum in hoc versetur, ut demonstretur, proposito quocunque numero primo, vel formae $8n+1$, vel formae $8n+3$, semper dari numerum $2aa+bb$ per eum divisibilem, ita ut radices a et b sint numeri inter se primi, operam is perdiderit, qui valores numerorum a et b per n expressos, investigare voluerit, propterea quod hi numeri non tantum ab n pendent, sed etiam ea ratio, quod numerus $8n+1$, vel $8n+3$ sit primus, necessario in computum duci debeat. Nam si numerus $8n+1$, vel $8n+3$, non fuerit primus, evenire adeo potest, ut nullus numerus $2aa+bb$ per eum sit divisibilis. Jam equidem demonstravi, per numerum $8n+1$, si sit primus, divisibiles esse omnes numeros formae $p^{8n}-q^{8n}$, et per numerum primum $8n+3$ omnes numeros formae $p^{8n+2}-q^{8n+2}$; tum vero etiam semper ejusmodi dari numeros p et q, ut priori casu forma $p^{4n}+q^{4n}$ per $8n+1$, posteriori vero forma $p^{4n+1}+q^{4n+1}$ per $8n+3$ divisibilis existat. Demonstrandum igitur esset in his formis $p^{4n}+q^{4n}$ et $p^{4n+1}+q^{4n+1}$ necessario semper ejusmodi involvi casus, qui sint aggregata ex quadrato et duplo quadrato; quod autem quo modo demonstrari posset, nondum perspicio. Aeque difficile ergo, ac fortasse difficilius erit, sequentes propositiones demonstrare, quae tamen aeque certae videntur, excepta prima, cujus demonstrationem dedi.

I. Omnis numerus primus formae $4n+1$ in hac forma $aa+bb$ continetur.

II. Omnes numeri primi in his formis $8n+1$ et $8n+3$ contenti, simul in hac forma continentur $2aa+bb$.

III. Omnes numeri primi vel hujus formae $12n+1$, vel hujus $12n+7$, seu hujus unicae $6n+1$, in hac forma $3aa+bb$ continentur.

IV. Omnes numeri primi in quapiam harum formularum

$$16n+1, \quad 16n+5, \quad 16n+9, \quad 16n+13,$$

vel in hac $4n+1$ contenti, simul sunt numeri formae $4aa+bb$, cujus quidem demonstratio jam in prima comprehenditur.

V. Omnes numeri primi in aliqua harum formularum contenti,

$$20n + 1, \quad 20n + 9,$$

simul quoque sunt formae $5aa + bb$.

VI. Omnes numeri primi in aliqua harum formularum contenti,

$$24n + 1, \quad 24n + 7,$$

simul quoque sunt formae $6aa + bb$.

VII. Omnes numeri primi in aliqua harum formularum contenti,

$$28n + 1, \quad 28n + 9, \quad 28n + 11, \quad 28n + 15, \quad 28n + 23, \quad 28n + 25,$$

vel, quod eodem redit, in harum aliqua:

$$14n + 1, \quad 14n + 9, \quad 14n + 11,$$

simul quoque sunt formae $7aa + bb$.

VIII. Omnes numeri primi in alterutra harum formularum contenti,

$$24n + 5 \quad \text{et} \quad 24n + 11,$$

simul sunt numeri formae $3aa + 2bb$.

Hujusmodi autem theorematum numerus quousque libuerit continuari potest.

Verum tamen in iis formandis probe cavendum est, ne inductioni nimis tribuatur: neque enim si fuerit numerus quispiam primus p in hac forma $faa + gbb$ contentus, inde generatim concludere licet, omnes numeros primos formae $4fgn + p$ fore numeros ejusdem formae $faa + gbb$, etiamsi hoc, si f et g fuerint numeri exigui, verum esse videatur. Etsi enim est $67 = 5.9 + 22.1$, ideoque formae $5aa + 22bb$, tamen numerus $4.5.22n + 67$, qui casu $n = 2$ est $= 40.22 + 67 = 947$ scilicet primus, non in forma $5aa + 22bb$ continetur: interim tamen affirmare licet, cum sit $23 = 5.2^2 + 3.1$, ideoque in forma $5aa + 3bb$ contineatur, omnes numeros primos $60n + 23$ in eadem forma contineri. Quodsi igitur quis methodum invenerit, hujusmodi theoremata tam inveniendi, quam, in quo caput rei est positum, demonstrandi, is certe in doctrina numerorum plurimum praestitisse erit judicandus.

Admissa autem hac proprietate numerorum primorum in his formulis $8n + 1$ et $8n + 3$ contentorum, plura alia hinc deduci poterunt egregia theoremata, quorum quaedam notasse juvabit.

57. **Theorema 12.** Si numerus quicunque in alterutra harum formularum $8n + 1$, vel $8n + 3$, contentus, nullo modo in formam $2aa + bb$ resolvi possit, tum non erit primus; at si unico modo in hanc formam possit resolvi, tum erit primus; sin autem plus uno modo haec resolutio succedat, tum pariter non erit primus, sed compositus.

Demonstratio. Pars secunda et tertia ex jam demonstratis sunt manifestae. Si enim numerus propositus unico modo in forma $2aa + bb$ contineatur, tum certe est primus, sin pluribus, compositus. Quod autem ad partem primam attinet, ea vi proprietatis nondum demonstratae subsistit; nam si numerus propositus esset primus, in formam $2aa + bb$ resolvi posset, quando ergo hanc resolutionem non admittit, tum certo non est primus. Q. E. D.

58. **Coroll. 1.** Hinc igitur patet modus non difficilis propositum numerum, si fuerit vel formae $8n + 3$, vel $8n + 1$, explorandi, utrum sit primus, nec ne? Subtrahantur enim ab eo successive omnia quadrata duplicata, scilicet:

2, 8, 18, 32, 50, 72, 98, etc.

quorum differentiae constituunt progressionem arithmeticam:

6, 10, 14, 18, 22, 26, etc.

et dispiciatur, utrum uspiam quadratum relinquatur.

59. **Coroll. 2.** Possunt etiam plures operationes simul institui, ac primo successive subtrahi haec quadrata duplicata:

2, 72, 242, 512, 882, etc., quorum differentiae sunt 70, 170, 270, 370, etc.

secundo vero haec quadrata duplicata:

8, 98, 288, 578, 968, etc., quorum differentiae sunt 90, 190, 290, 390, etc.

tertio haec:

18, 128, 338, 648, 1058, etc., quorum differentiae sunt 110, 210, 310, 410, etc.

quarto haec:

32, 162, 392, 722, 1152, etc., quorum differentiae sunt 130, 230, 330, 430, etc.

quinto haec:

50, 200, 450, 800, 1250, etc., quorum differentiae sunt 150, 250, 350, 450, etc.

ubi ex figuris finalibus mox patebit, quaenam operationes sint inutiles.

60. **Coroll. 3.** A numeris autem formae $8n+1$ quadrata tantum paria duplicata subtrahi debent, unde exclusis quadratis imparibus duplicatis, sequentes numeri erunt subtrahendi:

I. 8, 288, 968, 2048, etc.
280, 680, 1080,
400, 400.

II. 32, 392, 1152, 2312, etc.
360, 760, 1160,
400, 400.

III. 0, 200, 800, 1800, etc.
200, 600, 1000,
400, 400.

IV. 72, 512, 1352, 2592, etc.
440, 840, 1240,
400, 400.

V. 128, 648, 1568, 2888, etc.
520, 920, 1320,
400, 400.

61. **Coroll. 4.** Sin autem numerus sit formae $8n+3$, tum tantum quadrata imparia duplicata subtrahi debent, quae sunt:

I. 2, 242, 882, 1922, etc.
240, 640, 1040,
400, 400.

II. 18, 338, 1058, 2178, etc.
320, 720, 1120,
400, 400.

III. 50, 450, 1250, 2450, etc.
400, 800, 1200,
400, 400.

IV. 98, 578, 1458, 2738, etc.
480, 880, 1280,
400, 400.

V. 162, 722, 1682, 3042, etc.
560, 960, 1360,
400, 400.

62. *Exempl.* 1. Exploretur numerus 67579, utrum sit primus, nec ne?

Cum hic numerus contineatur in forma $8n + 3$, subtrahantur numerorum ordines ex coroll. 4, isque tantum secundus, tertius ac quartus, quia primus et quintus darent notam finalem 7, quae quadrato repugnat.

II. 67579		III. 67579		IV. 67579	
18		50		98	
67561	50281	67529	49529	67481	48761
320	3920	400	4000	480	4080
67241	46361	67129	45529	67001	44681
720	4320	800	4400	880	4480
66521	42041	66329	41129	66121	40201
1120	4720	1200	4800	1280	4880
65401	37321	65129	36329	64841	35321
1520	5120	1600	5200	1680	5280
63881	32201	63529	31129	63161	30041
1920	5520	2000	5600	2080	5680
61961	26681	61529	25529	61081	24361
2320	5920	2400	6000	2480	6080
59641	20761	59129	19529	58601	18281
2720	6320	2800	6400	2880	6480
56921	14441	56329	13129	55721	11801
3120	6720	3200	6800	3280	6880
53801	7721	53129	6329	* 229 52441	4921
3520	7120	3600		3680	
50281	601	49529		48761	

Hic unicum occurrit quadratum $52441 = 229^2$, ut sit $67579 = 2.87^2 + 229^2$, ideoque primus.

63. *Exempl.* 2. Exploretur numerus 40081, utrum sit primus, nec ne?

Cum hic numerus contineatur in forma $8n + 1$, subtrahantur numeri coroll. 3, eorumque quidem ordines II, III et IV, hoc modo:

II. 40081		III. 40081		IV. 40081	
32		200		72	
40049	29129	39881	27281	40009	28529
360	3160	600	3400	440	3240
39689	25969	39281	23881	39569	25289
760	3560	1000	3800	840	3640
38929	22409	38281	20081	38729	21649
1160	3960	1400	4200	1240	4040
37769	18449	36881	15881	37489	17609
1560	4360	1800	4600	1640	4440
36209	14089	35081	11281	35849	13169
1960	4760	2200	5000	2040	4840
34249	9329	32881	6281	33809	8329
2360	5160	2600	5400	2440	5240
31889	4169	30281	881	31369	3089
2760		3000		2840	
29129		27281		28529	

quia igitur hic nusquam quadratum remansit, numerus propositus non est primus, est vero productum

$= 149.269.$

64. **Theorema 13.** Si numerus n nullo modo sit aggregatum ex numero quadrato et trigonali, tum numerus $8n+1$ certe non erit primus.

Demonstratio. Si enim n nullo modo in hac forma $aa+\frac{1}{2}(bb+b)$ contineatur, tum $8n+1$ nullo modo in hac forma $8aa+4bb+4b+1$ continetur, non ergo erit numerus formae $2pp+qq$, ideoque non erit primus. Q. E. D.

65. **Coroll.** At si n unico modo sit aggregatum ex quadrato et trigonali, tum $8n+1$ certe erit numerus primus; sin autem sit pluribus modis, non erit primus, sed compositus.

66. **Theorema 14.** Si numerus n nullo modo fuerit aggregatum ex numero trigonali et trigonali duplicato, tum $8n+3$ certe non erit primus.

Demonstratio. Si enim n nullo modo in hac forma $aa+a+\frac{1}{2}(bb+b)$ contineatur, tum $8n+3$ nullo modo in hac forma $8aa+8a+2+4bb+4b+1$, ideoque nec in hac $2pp+qq$ continebitur, consequenter non erit primus. Q. E. D.

67. **Coroll.** At si n unico modo fuerit aggregatum ex trigonali et trigonali duplicato, tum $8n+3$ certe erit primus; sin autem fuerit plus uno modo, compositus.



XIV.

Solutio generalis quorundam problematum Diophanteorum, quae vulgo nonnisi solutiones speciales admittere videntur.

(N. Comment. VI. 1756—57. p. 155. Exhib. 1754. Sept. 30.)

1. Analysis Diophantea, quae in problematibus indeterminatis per numeros rationales vel etiam integros solvendis versatur, duplicis generis problemata tractare solet, quorum discrimen in ratione solutionis maxime est positum. Alia enim problemata ita sunt comparata, ut solutiones generales exhiberi queant, quae omnes plane numeros satisfacientes in se complectuntur: alia vero nonnisi solutiones particulares admittunt, vel saltem per methodos cognitas nonnisi tales solutiones eruere licet, ita ut praeter numeros, qui forte reperiuntur, infiniti alii problemati satisfacientes existant, qui in solutione inventa non contineantur. Ubi quidem in genere notari convenit, prioris ordinis problemata multo facilius resolvi, quam ea, quae ad alterum ordinem referuntur, quippe quae plerumque singularem sagacitatem cum eximiis artificiis conjunctam requirunt, in quibus maxima vis hujus analysis cernitur. Quare ob hanc causam problemata Diophantea in has duas classes distribui debere videntur.

2. Diophantus quidem ipse omnium quaestionum, quas tractat, solutiones tantum specialissimas tradit, numerosque, quibus unica solutio continetur, plerumque indicasse est contentus. Neque vero ejus methodus ad has solutiones specialissimas adstricta est putanda; quia enim tunc temporis usus litterarum, quibus numeri indefiniti designentur, nondum erat receptus, hujusmodi solutiones latius patentes, quales nunc quidem exhiberi solent, ab ipso expectari non poterant; interim tamen ipsae methodi, quibus ad quaelibet problemata solvenda utitur, aeque late patent, quam eae, quae hodie sunt in usu: quin etiam fateri cogimur, vix ullam in hoc analyseos genere adhuc esse inventam, cujus vestigia satis luculenta non jam in ipso Diophanto deprehendantur. Non obstante igitur hac apparente particularitate solutionum Diophantearum, disparitas problematum supra memorata, in ipso jam Diophanto manifesto cernitur, siquidem ad methodos ejus respiciamus: quarum aliae ita sunt comparatae, ut omnes omnino solutiones, quae problemati satisfacere possunt, suppeditare queant, aliae vero nonnullas tantum solutiones praebeant, vel etiamsi earum numerus in infinitum augeri possit, tamen in iis innumerabiles aliae, quae aeque satisfaciunt, non contineantur.

3. Exemplum problematis, cujus solutio generalis exhiberi potest, praebet quaestio vulgata, qua quaeruntur duo numeri quadrati, quorum summa sit quadratum; sive sumtis x et y pro radicibus istorum quadratorum, ut $xx+yy$ sit numerus quadratus. Sumtis enim pro lubitu tribus numeris a, p et q, haec habebitur solutio generalis: $y=2apq$ et $x=a(pp-qq)$; ex his namque valoribus prodit $\sqrt{(xx+yy)}=a(pp+qq)$. De qua solutione tenendum est, nullos plane dari numeros pro x et y substituendos, quorum quadratorum summa fiat quadratum, qui non simul in formulis datis contineantur. Atque haec generalitas non solum inde perspicitur, quod pro tribus

litteris a, p et q numeros quoscunque accipere liceat, unde jam infinities infinita solutionum multitudo obtinetur; sed etiam ipsa harum formularum investigatio evincit, nullam plane dari solutionem, quae non in iis comprehendatur. At vero hoc posterius criterium longe certius est priori, cum saepe multae litterae indefinitae in solutionem ingredi queant, neque tamen solutio propterea reddatur generalis.

4. Investigationis autem ratio in hoc exemplo nobis solutionis universalitatem plane ostendit: cum enim $\sqrt{(xx+yy)}$ debeat esse numerus rationalis, is certe erit major quam x; statuatur ergo $= x + z$. Tum vero quaecunque sit ratio ipsius y ad z, poni poterit $z = \frac{q}{p}y$, neque hoc modo generalitas positionis limitatur. Posito autem $\sqrt{(xx+yy)} = x + \frac{q}{p}y$ sumtis quadratis habebimus: $xx + yy = xx + \frac{2q}{p}xy + \frac{qq}{pp}yy$. Deleto utrinque termino xx, ac residuo per y diviso, prodibit

$$y = \frac{2q}{p}x + \frac{qq}{pp}y, \quad \text{seu} \ (pp - qq)y = 2pqx.$$

Erit ergo $\frac{x}{y} = \frac{pp-qq}{2pq}$, hincque x et y sunt vel aeque multipla, vel aeque submultipla numerorum $pp - qq$ et $2pq$. Sumta ergo a pro indice generali sive multiplorum, sive submultiplorum, nanciscemur $y = 2apq$ et $x = a(pp-qq)$, et ob $z = \frac{q}{p}y = 2aqq$, erit $x + z = \sqrt{(xx+yy)} = a(pp+qq)$.

5. Problematis autem, cujus solutio per methodos cognitas generalis exhiberi nequit, exemplum esto quaestio de inveniendis tribus cubis quorum summa sit cubus; sive quaerendi sint tres numeri x, y et z ita, ut sit $x^3 + y^3 + z^3 =$ cubo. Quod problema cum ab ipso Diophanto, tum a recentioribus, pluribus modis extat solutum, atque ita quidem, ut infinita multitudo solutionum sit exhibita; neque tamen ulla solutio tam late patet, ut omnes plane casus huic quaestioni satisfacientes in se complectatur. In hoc problemate etiam vel unus cubus x^3, vel duo x^3 et y^3, tanquam dati spectari possunt, unde vel duos reliquos cubos, vel unicum quaeri oportet, ut summa fiat cubus: quomodocunque autem solutio instituatur, tamen maxime particularis evadit.

6. Quod quo clarius perspiciatur, solutiones dari solitas hic breviter commemoremus. Sint igitur primo dati duo cubi a^3 et b^3, tertiumque x^3 inveniri oporteat, ut omnium trium summa $a^3 + b^3 + x^3$ denuo fiat cubus: Manifestum jam quidem est, radicem hujus cubi majorem fore quam x; sed etiamsi statuatur $= x + v$, tamen aequatio quadratica pro inveniendo x prodit, sicque difficultas non diminuitur. Poni igitur solet $x = p - b$, ut summa trium cuborum fiat:

$$a^3 + 3bbp - 3bpp + p^3 = \text{cubo} = v^3$$

atque hac quidem positione amplitudo solutionis non restringitur. Porro autem ejusmodi cubus assumi debet, ut incognita p per aequationem simplicem, ideoque rationaliter exhiberi queat. Manifestum autem est hoc duplici modo fieri posse: primo enim sumto $v = a + p$, fiet

$$a^3 + 3bbp - 3bpp + p^3 = a^3 + 3aap + 3app + p^3,$$

ubi cum termini a^3 et p^3 se destruant, reliquum per $3p$ divisum dat:

$$bb - bp = aa + ap, \quad \text{ideoque} \ p = \frac{bb-aa}{a+b} = b - a,$$

unde fit $x = p - b = -a$, quo casu utique fit:

$$a^3 + b^3 + x^3 = a^3 + b^3 - a^3 = b^3 = \text{cubo}.$$

7. Hanc autem solutionem maxime particularem esse, ex assumtione valoris $v=a+p$ evidens est, cum ubique fieri possit, ut quantitas $a^3+3bbp-3bpp+p^3$ sit cubus, cujus radix non sit $a+p$, ita ut hac restrictione solutio maxime sit limitata, unde factum est, ut etiam unicum valorem pro p, ac proinde pro x exhibuerit, qui adeo ne solutionem quidem idoneam suppeditasse est censendus, propterea quod invenimus $x=-a$, qui casus tam est obvius sua sponte, ut ne pro solutione quidem admitti queat. Pro v igitur alius valor fingi solet, talis tamen, ut inventio ipsius p ad aequationem simplicem perducat, quod usu venit ponendo $v=a+\frac{bb}{aa}p$; fiet enim:

$$a^3+3bbp-3bpp+p^3=a^3+3bbp+\frac{3b^4}{a^3}pp+\frac{b^6}{a^6}p^3,$$

quae utrinque deletis terminis a^3+3bbp, per pp divisa dat:

$$-3b+p=\frac{3b^4}{a^3}+\frac{b^6}{a^6}p, \quad \text{seu} \quad p=\frac{3a^6b+3a^3b^4}{a^6-b^6}.$$

8. Cum igitur hinc invenerimus

$$p=\frac{3a^3b(a^3+b^3)}{a^6-b^6}=\frac{3a^3b}{a^3-b^3}, \quad \text{erit} \quad x=p-b=\frac{2a^3b+b^4}{a^3-b^3}=\frac{b(2a^3+b^3)}{a^3-b^3},$$

quae est radix tertii cubi ad duos datos a^3+b^3 addendi, ut summa fiat cubus. Erit autem summae radix cubica per hypothesin

$$=v=a+\frac{bb}{aa}p=a+\frac{3ab^3}{a^3-b^3}, \quad \text{sive} \quad v=\frac{a^4+2ab^3}{a^3-b^3}=\frac{a(a^3+2b^3)}{a^3-b^3}.$$

Quicunque ergo numeri pro a et b fuerint assumti, hinc habebuntur tres cubi, quorum summa est cubus. Hi scilicet erunt:

$$a^3+b^3+\left(\frac{b(2a^3+b^3)}{a^3-b^3}\right)^3=\left(\frac{a(a^3+2b^3)}{a^3-b^3}\right)^3.$$

Verum et hanc solutionem maxime esse specialem ex ipsa investigatione perspicuum est, cum plane pro arbitrio nostro radicem trium cuborum finxerimus $v=a+\frac{bb}{aa}p$, cum sine dubio infinitos quoque alios valores recipere possit.

9. Porro autem datis duobus cubis unicus reperitur tertius cubus, qui cum iis conjunctus producat cubum; manifestum autem est, infinitos hujusmodi dari cubos. Si enim sit $a=4$ et $b=3$, radix tertii cubi hinc prodit

$$x=\frac{3(2.64+27)}{64-27}=\frac{465}{37}, \quad \text{et} \quad v=\frac{472}{37}, \quad \text{ita ut sit} \quad 4^3+3^3+\left(\frac{465}{37}\right)^3=\left(\frac{472}{37}\right)^3.$$

Novimus autem cubum quinarii ad hos cubos 4^3+3^3 additum quoque producere cubum scilicet senarii, seu esse $3^3+4^3+5^3=6^3$, qui tamen casus in hac solutione non continetur. Quare si ad hoc problema solvendum, ut sit $x^3+y^3+z^3=v^3$, quis dicat sumi debere:

$$x=a; \quad y=b \quad \text{et} \quad z=\frac{b(2a^3+b^3)}{a^3-b^3}$$

tumque fore $v=\frac{a(a^3+2b^3)}{a^3-b^3}$, hae formulae quidem satisfaciunt, sed etiamsi, ob duos numeros a et b arbitrio nostro relictos, infinities infiniti cuborum terniones hinc exhiberi possint, quorum summa faciat cubum, tamen infiniti alii existunt cuborum terniones idem praestantes, qui in istis formulis non sunt contenti; veluti hic casus $x=3$, $y=4$ et $z=5$, pro quo fit $v=6$.

10. Latius quidem patens reperitur solutio, si unicus tantum trium cuborum quasi datus assumatur, ita ut fieri oporteat $a^3+x^3+y^3=v^3$. Ponatur hunc in finem $x=pu+r$ et $y=qu-r$, qua quidem positione nulla restrictio inducitur, fietque

$$a^3+3rr(p+q)u+3r(pp-qq)uu+(p^3+q^3)u^3=v^3.$$

Jam ut quantitas u hinc rationaliter definiri queat, fingatur $v=a+\frac{rr}{aa}(p+q)u$, qua positione utique solutio jam vehementer limitatur: ex ea autem obtinebitur:

$$v^3=a^3+3rr(p+q)u+\frac{3r^4}{a^3}(p+q)^2uu+\frac{r^6}{a^6}(p+q)^3u^3.$$

Deletis ergo utrinque terminis $a^3+3rr(p+q)u$, et residuo per $(p+q)uu$ diviso, emerget haec aequatio:

$$3r(p-q)+(pp-pq+qq)u=\frac{3r^4}{a^3}(p+q)+\frac{r^6}{a^6}(p+q)^2u,$$

ex qua eruitur:
$$u=\frac{3a^3r^4(p+q)-3a^6r(p-q)}{a^6(pp-pq+qq)-r^6(p+q)^2}.$$

11. Valore ergo hoc pro u invento, erit

$$x=pu+r=\frac{3a^3pr^4(p+q)-a^6r(2pp-2pq-qq)-r^7(p+q)^2}{a^6(pp-pq+qq)-r^6(p+q)^2}$$

$$y=qu-r=\frac{3a^3qr^4(p+q)-a^6r(pp+2pq-2qq)+r^7(p+q)^2}{a^6(pp-pq+qq)-r^6(p+q)^2}$$

et
$$v=a+\frac{rr}{aa}(p+q)u=\frac{a^7(pp-pq+qq)-3a^4r^3(pp-qq)+2ar^6(p+q)^2}{a^6(pp-pq+qq)-r^6(p+q)^2}.$$

Cum igitur quatuor litterae a, p, q et r pro arbitrio assumi queant, haec solutio utique infinities latius patet, quam praecedens, ubi duae tantum litterae arbitrio nostro relinquebantur. Verum tamen notandum est, rationem tantum litterarum p et q in computum ingredi, ita ut hinc litterae arbitrariae ad tres tantum reducantur: nihilo vero minus et haec solutio, ob limitationem circa radicem v adhibitam, pro particulari est habenda, ita ut terniones cuborum existant in his formulis non contenti. Solutio autem antecedens ex hac emergit, sumto $p=0$, ita ut haec infinities illa sit generalior.

12. Adhuc generaliorem autem obtinebimus, si nullum trium cuborum tanquam cognitum assumamus, seu in genere quaeramus x, y et z, ut sit $x^3+y^3+z^3=v^3$. In hunc finem ponatur

$$x=pt+u,\quad y=-pt+qu\quad\text{et}\quad z=t-qu,$$

quibus positionibus nihil adhuc limitatur: facta autem substitutione, oritur

$$\left.\begin{array}{l} t^3+3ppttu+3ptuu+u^3\\ +3ppqttu-3pqqtuu\\ -3qttu+3qqtuu\end{array}\right\}=v^3.$$

Jam fingatur $v=t+u$, unde quidem maxima limitatio nascitur, et aequatione per $3tu$ divisa, reperietur:
$$(pp+ppq-q)t+(p-pqq+qq)u=t+u,$$

seu
$$\frac{t}{u}=\frac{-1+p+qq-pqq}{1+q-pp-ppq}:$$

capi ergo poterit:

$$t=n\,(-pqq+qq+p-1) \quad \text{et} \quad u=n\,(-ppq-pp+q+1)$$

unde elicitur:

$$\begin{aligned} x&=n\,(-ppqq+pqq-ppq-p+q+1)\\ y&=n\,(p+q-pp+qq-ppq-pqq)\\ z&=n\,(+ppqq-pqq+ppq+p-q-1)\\ v&=n\,(-pqq-ppq-pp+qq+p+q). \end{aligned}$$

Hinc autem fit $z=-x$ et $v=y$, qui est casus per se obvius.

13. Sequenti autem modo solutio latius patens eruitur: Ponatur

$$x=mt+pu;\quad y=nt+qu \quad \text{et} \quad z=-nt+ru,$$

eritque

$$x^3+y^3+z^3=m^3t^3+\left.\begin{array}{r}3mmp\\+\ 3nnq\\+\ 3nnr\end{array}\right\}ttu \quad \left.\begin{array}{r}+3mpp\\+3nqq\\-3nrr\end{array}\right\}tuu \quad \left.\begin{array}{r}+p^3\\+q^3\\+r^3\end{array}\right\}u^3,$$

quae summa cum debeat esse cubus $=v^3$, ponatur:

$$v=mt+\frac{mmp+nn\,(q+r)}{mm}u;$$

eritque dividendo per uu

$$3t\,(mpp+n\,(qq-rr))+u\,(p^3+q^3+r^3)=\frac{3t}{m^3}(mmp+nn\,(q+r))^2+\frac{u}{m^6}(mmp+nn\,(q+r))^3,$$

sicque neglecto communi factore, qui ab arbitrio nostro pendet, erit

$$\begin{aligned} t&=m^6\,(p^3+q^3+r^3)-(mmp+nn\,(q+r))^3\\ u&=3m^3\,(mmp+nn\,(q+r))^2-3m^6\,(mpp+n\,(qq-rr)), \end{aligned}$$

quae formae si denuo per communem factorem $q+r$ dividantur, prodit

$$\begin{aligned} t&=m^6\,(qq-qr+rr)-3m^4nnpp-3mmn^4p\,(q+r)-n^6\,(q+r)^2\\ u&=-3m^6n\,(q-r)+6m^5nnp+3m^3n^4\,(q+r). \end{aligned}$$

14. Hinc jam pro x, y, z emergunt sequentes expressiones:

$$x=m^7(qq-qr+rr)-3m^6np(q-r)+3m^5nnpp-mn^6(q+r)^2,$$
$$y=-m^6n(2qq-2qr-rr)+6m^5nnpq-3m^4n^3pp+3m^3n^4q(q+r)-3mmn^5p(q+r)-n^7(q+r)^2,$$
$$z=+m^6n(-qq-2qr+2rr)+6m^5nnpr+3m^4n^3pp+3m^3n^4r(q+r)+3mmn^5p(q+r)+n^7(q+r)^2,$$

quorum cuborum summa iterum est cubus radicem habens v, ut sit

$$v=m^7(qq-qr+rr)-3m^6np(q-r)+3m^5nnpp-3m^4n^3(qq-rr)+6m^3n^4p(q+r)+2mn^6(q+r)^2.$$

Hi vero numeri etiam sequenti modo exhiberi possunt:

$$x=+3m^5n^2pp-3m^6npq+3m^6npr+\left.\begin{array}{r}m^7\\-mn^6\end{array}\right\}qq \quad \left.\begin{array}{r}-\quad m^7\\-2mn^6\end{array}\right\}qr \quad \left.\begin{array}{r}+\ m^7\\-mn^6\end{array}\right\}rr,$$

$$y=-3m^4n^3pp+\left.\begin{array}{r}6m^5n^2\\-3m^2n^5\end{array}\right\}pq \quad -3m^2n^5pr\left.\begin{array}{r}-2m^6n\\+3m^3n^4\\-\ n^7\end{array}\right\}qq \quad \left.\begin{array}{r}+2m^6n\\+3m^3n^4\\-2n^7\end{array}\right\}qr \quad \left.\begin{array}{r}+m^6n\\-\ n^7\end{array}\right\}rr,$$

$$z = +3m^4n^3pp + 3m^3n^4pq + \left.\begin{matrix} 6m^5n^2 \\ +3m^2n^5 \end{matrix}\right\} pr \left.\begin{matrix} -m^6n \\ +n^7 \end{matrix}\right\} qq \left.\begin{matrix} -2m^6n \\ +3m^3n^4 \\ +2n^7 \end{matrix}\right\} qr \left.\begin{matrix} +2m^6n \\ +3m^3n^4 \\ +n^7 \end{matrix}\right\} rr,$$

$$v = 3m^5n^2pp \left.\begin{matrix} -3m^6n \\ +6m^3n^4 \end{matrix}\right\} pq \left.\begin{matrix} +3m^6n \\ +6m^3n^4 \end{matrix}\right\} pr \left.\begin{matrix} +m^7 \\ -3m^4n^3 \\ +2mn^6 \end{matrix}\right\} qq \left.\begin{matrix} -m^7 \\ +4mn^6 \end{matrix}\right\} qr \left.\begin{matrix} +m^7 \\ +3m^4n^3 \\ +2mn^6 \end{matrix}\right\} rr.$$

Quibus valoribus substitutis actu fit $x^3 + y^3 + z^3 = v^3$.

15. Si singuli hi numeri insuper per coefficientem indefinitum multiplicentur, hae formulae continebunt sex litteras ab arbitrio nostro pendentes, quae quidem ad quatuor reducentur, unde eae latissime patere, omnesque omnino casus in se complecti videntur, verum tamen ex ipsa solutione, qua ipsi v valorem a litteris x, y et z pendentem tribuimus, perspicitur has formulas non nisi pro particularibus haberi posse. Ceterum quoque per alias positiones aliae eruuntur solutiones, quae pro certis casibus magis sint futurae idoneae; tum etiam methodus habetur ex inventa solutione quacunque particulari alias solutiones particulares eliciendi. His tamen omnibus artificiis, nisi in infinitum reiterentur, nulla solutio, quae pro generali haberi queat, obtineri potest. Quin etiam in universum fere adhuc est creditum, hujus generis problemata natura sua ita esse comparata, ut solutionem generalem prorsus non admittant, ex quo sequens istius problematis solutio, quae revera est generalis, imprimis notatu digna et finibus analyseos Diophanteae promovendis apta videtur.

16. **Problema.** *Invenire generatim omnes cuborum terniones, quorum summa sit cubus.*

Solutio. Sint A, B, C radices ternorum cuborum, et D radix cubica summae eorum; ita ut sit $A^3 + B^3 + C^3 = D^3$, cui aequationi haec forma tribuatur: $A^3 + B^3 = D^3 - C^3$. Ponatur jam

$$A = p + q, \quad B = p - q, \quad C = r - s \quad \text{et} \quad D = r + s,$$

qua positione amplitudo solutionis neutiquam restringitur. Hinc autem fit:

$$A^3 + B^3 = 2p^3 + 6pqq \quad \text{et} \quad D^3 - C^3 = 2s^3 + 6rrs$$

sicque erit:

$$p(pp + 3qq) = s(ss + 3rr),$$

quae aequatio subsistere nequit, nisi $pp + 3qq$ et $ss + 3rr$ communem habeant divisorem. Constat autem tales numeros alios non habere divisores, nisi qui ejusdem sint formae: quod ut obtineatur, loco quatuor litterarum p, q, r et s, aliae sex novae introducantur, hoc modo:

$$p = ax + 3by, \qquad s = 3cy - dx,$$
$$q = bx - ay, \qquad r = dy + cx,$$

unde multo minus amplitudini solutionis vis infertur. Hinc autem erit:

$$pp + 3qq = (aa + 3bb)(xx + 3yy) \quad \text{et} \quad ss + 3rr = (dd + 3cc)(xx + 3yy)$$

ac nostra aequatio per $xx + 3yy$ divisa induet sequentem formam:

$$(ax + 3by)(aa + 3bb) = (3cy - dx)(dd + 3cc),$$

qua id jam sumus consecuti, ut litterae x et y unicam tantum obtineant dimensionem, ideoque rationaliter definiri queant. Cum enim sit:

$$\frac{x}{y}=\frac{-3b\,(aa+3bb)+3c\,(dd+3cc)}{a\,(aa+3bb)+d\,(dd+3cc)},$$

ponatur

$$x=-3nb\,(aa+3bb)+3nc\,(dd+3cc),$$
$$y=na\,(aa+3bb)+nd\,(dd+3cc).$$

Ex quibus valoribus litterae p, q, r, s ita definiuntur, ut sit:

$$p=3n\,(ac+bd)\,(dd+3cc),$$
$$q=n\,(3bc-ad)\,(dd+3cc)-n\,(aa+3bb)^2,$$
$$r=n\,(dd+3cc)^2-n\,(3bc-ad)\,(aa+3bb),$$
$$s=3n\,(ac+bd)\,(aa+3bb).$$

Atque hinc tandem radices cuborum quaesitorum A, B, C, D erunt:

$$A=n\,(3ac+3bc-ad+3bd)\,(dd+3cc)-n\,(aa+3bb)^2,$$
$$B=n\,(3ac-3bc+ad+3bd)\,(dd+3cc)+n\,(aa+3bb)^2,$$
$$C=n\,(dd+3cc)^2-n\,(3ac+3bc-ad+3bd)\,(aa+3bb),$$
$$D=n\,(dd+3cc)^2+n\,(3ac-3bc+ad+3bd)\,(aa+3bb),$$

quibus valoribus obtinetur, ut sit:

$$A^3+B^3+C^3=D^3$$

et cum solutio nulla restrictione sit limitata, utique latissime patet omnesque cuborum terniones complectitur, quorum summa iterum est cubus.

17. **Coroll. 1.** Derivemus hinc formulas magis speciales, ac primo quidem sit $d=0$; eritque

$$A=9n\,(a+b)\,c^3-n\,(aa+3bb)^2,$$
$$B=9n\,(a-b)\,c^3+n\,(aa+3bb)^2,$$
$$C=9nc^4-3nc\,(a+b)\,(aa+3bb),$$
$$D=9nc^4+3nc\,(a-b)\,(aa+3bb).$$

Si hic ulterius ponatur $b=a$, fiet

$$A=18nac^3-16na^4,\quad B=16na^4,\quad C=9nc^4-24na^3c\quad \text{et}\quad D=9nc^4,$$

sin autem fiat $b=-a$, eruetur

$$A=-16na^4,\quad B=18nac^3+16na^4,\quad C=9nc^4,\quad \text{et}\quad D=9nc^4+24na^3c.$$

18. **Coroll. 2.** Ponamus nunc $c=0$, eritque

$$A=n\,(3b-a)\,d^3-n\,(aa+3bb)^2,$$
$$B=n\,(3b+a)\,d^3+n\,(aa+3bb)^2,$$
$$C=nd^4-nd\,(3b-a)\,(aa+3bb),$$
$$D=nd^4+nd\,(3b+a)\,(aa+3bb).$$

Si ulterius ponatur $b=a$, erit

$$A=2nad^3-16na^4,\quad B=4nad^3+16na^4,\quad C=nd^4-8na^3d,\quad D=nd^4+16na^3d.$$

Sin autem fiat $a=-b$, erit

$$A=4nbd^3-16nb^4,\quad B=2nbd^3+16nb^4,\quad C=nd^4-16nb^3d,\quad D=nd^4+8nb^3d.$$

19. **Coroll. 3.** Si nunc $b = 0$, formulaeque nostrae fient:

$$A = na(3c - d)(dd + 3cc) - na^4,$$
$$B = na(3c + d)(dd + 3cc) + na^4,$$
$$C = n(dd + 3cc)^2 - na^3(3c - d),$$
$$D = n(dd + 3cc)^2 + na^3(3c + d).$$

Quod si jam praeterea statuatur $d = c$, erit

$$A = 8nac^3 - na^4, \quad B = 16nac^3 + na^4, \quad C = 16nc^4 - 2na^3c, \quad D = 16nc^4 + 4na^3c,$$

sin autem fiat $d = -c$, erit

$$A = 16nac^3 - na^4, \quad B = 8nac^3 + na^4, \quad C = 16nc^4 - 4na^3c, \quad D = 16nc^4 + 2na^3c.$$

20. **Coroll. 4.** Ponatur denique $a = 0$, atque obtinebimus:

$$A = 3nb(c + d)(dd + 3cc) - 9nb^4,$$
$$B = 3nb(d - c)(dd + 3cc) + 9nb^4,$$
$$C = n(dd + 3cc)^2 - 9nb^3(c + d),$$
$$D = n(dd + 3cc)^2 + 9nb^3(d - c).$$

Si ulterius ponatur $d = c$, erit

$$A = 24nbc^3 - 9nb^4, \quad B = 9nb^4, \quad C = 16nc^4 - 18nb^3c, \quad D = 16nc^4,$$

sin autem sit $c = -d$, habebitur

$$A = -9nb^4, \quad B = 24nbd^3 + 9nb^4, \quad C = 16nd^4, \quad D = 16nd^4 + 18nb^3d.$$

21. **Coroll. 5.** Si numerorum A, B, C unus fiat negativus, quod pro lubitu effici potest, veluti si fiat $A = -E$, erit $B^3 + C^3 = D^3 + E^3$, sicque simul hoc problema generalissime dedimus solutum, quo bina cuborum paria quaeruntur, quorum summae sint inter se aequales. Sin autem duae radices prodeant negativae, veluti

$$A = -E \quad \text{et} \quad B = -F, \quad \text{erit} \quad C^3 = D^3 + E^3 + F^3,$$

sicque denuo nostri problematis solutio habebitur.

22. **Scholion 1.** Formulae specialissimae, in his corollariis exhibitae, ad binas has reducuntur, siquidem in coroll. 3 pro a scribatur $2a$ et $n = \frac{n}{16}$, et in coroll. 1, $\frac{1}{2}a$ pro a:

$$\begin{aligned} A &= nac^3 - na^4 & \qquad A &= 9nac^3 - na^4 \\ B &= 2nac^3 + na^4 & B &= na^4 \\ C &= nc^4 - na^3c & C &= 9nc^4 - 3na^3c \\ D &= nc^4 + 2na^3c & D &= 9nc^4, \end{aligned}$$

quarum prior convenit cum supra § 8 inventa, altera autem praebet hunc casum simplicissimum

$$A = 8, \quad B = 1, \quad C = 6 \quad \text{et} \quad D = 9, \quad \text{ita ut sit} \quad 1^3 + 6^3 + 8^3 = 9^3.$$

23. **Scholion 2.** Primo intuitu formulae generales in problemate erutae non latius patere videntur, quam formulae supra § 14 exhibitae, cum utrinque quinque insint litterae arbitrariae, atque istae insuper coefficientem communem recipere queant, ita ut etiam magis generales videantur.

Interim tamen ipsa solutionis ratio declarat, formulas in problemate inventas esse amplissimas, dum superiores insigni restrictione sunt limitatae. Quae restrictio quo clarius perspiciatur, ex § 13 perpendatur positio

$$v = mt + \frac{mmp + nn(q+r)}{mm} u = mt + pu + \frac{nn}{mm}(q+r)u.$$

Jam vero est $mt + pu = x$ et $y + z = (q+r)u$, ita ut positio sit

$$v = x + \frac{nn}{mm}(y+z).$$

Quare, ut fiat $x^3 + y^3 + z^3 = v^3$, in illa solutione assumitur esse $\frac{v-x}{y+z} = \frac{nn}{mm} =$ quadrato; sicque illa ad alios casus non pateat, nisi in quibus sit $\frac{v-x}{y+z}$ seu $\frac{D-A}{B+C}$ numerus quadratus. Quoties igitur $\frac{D-A}{B+C}$ non fit quadratum, casus in superioribus formulis non continetur: hujusmodi autem casus dari, vel ex exemplo $1^3 + 6^3 + 8^3 = 9^3$ liquet, in quo neque $\frac{9-1}{6+8}$, neque $\frac{9-6}{1+8}$, neque $\frac{9-8}{1+6}$, fit quadratum. Solutio autem problematis tali restrictione non limitatur; cum sit

$$\frac{D-C}{A+B} = \frac{s}{p} = \frac{pp+3qq}{ss+3rr} = \frac{aa+3bb}{dd+3cc},$$

unde ex solutione generali ii tantum casus, quibus $\frac{aa+3bb}{dd+3cc}$ est numerus quadratus in formulis superioribus § 14 continentur; ex quo summa generalitas nostrae solutionis manifesto elucet.

24. **Scholion 3.** Natura autem hujus problematis numeros integros tantum postulat, et quidem tales, qui sint primi inter se; si enim fuerit $A^3 + B^3 + C^3 = D^3$, tum problemati quoque satisfacient omnia tam aeque multipla, quam aeque submultipla numerorum A, B, C, D; ideoque sufficiet, eos tantum notasse casus, quibus numeri A, B, C, D fiunt cum integri, tum primi inter se. Hunc in finem sumtis pro a, b, c, d numeris quibuscunque, sive affirmativis, sive negativis, inde primum formentur

$$x = 3n(c(dd+3cc) - b(aa+3bb)),$$
$$y = n(d(dd+3cc) + a(aa+3bb)),$$

ac pro n talis sumatur fractio, ut x et y fiant integri et primi inter se. Ex his porro formentur:

$$p = ax + 3by, \quad q = bx - ay, \quad r = dy + cx \quad \text{et} \quad s = 3cy - dx,$$

qui denuo per communem divisorem, si quem habent, deprimantur. Hinc denique habebitur

$$A = p + q, \quad B = p - q, \quad C = r - s \quad \text{et} \quad D = r + s,$$

sicque fiet $A^3 + B^3 + C^3 = D^3$. Atque casus, quibus unus horum numerorum fit negativus, simul omnes solutiones praebebunt, quibus summa duorum cuborum aequalis est summae duorum aliorum cuborum. In hoc calculo conveniet copiam numerorum formae $mm + 3nn$ in promtu habere, unde deinceps formulae $aa + 3bb$ et $dd + 3cc$ desumi queant.

Tabula numerorum formae $mm + 3nn$.

m	Numerus n: 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	3	12	27	48	75	108	147	192	243	300	363	432	507	588	675	768	867	972
1	1	4	13	28	49	76	109	148	193	244	301	364	433	508	589	676	769	868	973
2	4	7	16	31	52	79	112	151	196	247	304	367	436	511	592	679	772	871	976
3	9	12	21	36	57	84	117	156	201	252	309	372	441	516	597	684	777	876	981
4	16	19	28	43	64	91	124	163	208	259	316	379	448	523	604	691	784	883	988
5	25	28	37	52	73	100	133	172	217	268	325	388	457	532	613	700	791	892	997
6	36	39	48	63	84	111	144	183	228	279	336	399	468	543	624	711	802	903	
7	49	52	61	76	97	124	157	196	241	292	349	412	481	556	637	724	815	916	
8	64	67	76	91	112	139	172	211	256	307	364	427	496	571	652	739	830	931	
9	81	84	93	108	129	156	189	228	273	324	381	444	513	588	669	756	847	948	
10	100	103	112	127	148	175	208	247	292	343	400	463	532	607	688	775	866	967	
11	121	124	133	148	169	196	229	268	313	364	421	484	553	628	709	796	887	988	
12	144	147	156	171	192	219	252	291	336	387	444	507	576	651	732	819	910		
13	169	172	181	196	217	244	277	316	361	412	469	532	601	676	757	844	935		
14	196	199	208	223	244	271	304	343	388	439	496	559	628	703	784	871	962		
15	225	228	237	252	273	300	333	372	417	468	525	588	657	732	813	900	991		
16	256	259	268	283	304	331	364	403	448	499	556	619	688	763	844	931			
17	289	292	301	316	337	364	397	436	481	532	589	652	721	796	877	964			
18	324	327	336	351	372	399	432	471	516	567	624	687	756	831	912	999			
19	361	364	373	388	409	436	469	508	553	604	661	724	793	868	949				
20	400	403	412	427	448	475	508	547	592	643	700	763	832	907	988				
21	441	444	453	468	489	516	549	588	633	684	741	804	873	948					
22	484	487	496	511	532	559	592	631	676	727	784	847	916	991					
23	529	532	541	556	577	604	637	676	721	772	829	892	961						
24	576	579	588	603	624	651	684	723	768	819	876	939							
25	625	528	637	652	673	700	733	772	817	868	925	988							
26	676	679	688	703	724	751	784	823	868	919	976								
27	729	732	741	756	777	804	837	876	921	972									
28	784	787	796	811	832	859	892	931	976										
29	841	844	853	868	889	916	949	988											
30	900	903	912	927	948	975													
31	961	964	973	988															

25. **Scholion 4.** Ex hac tabula jam pro lubitu numeri pro $aa+3bb$ et $dd+3cc$ assumi poterunt, unde valores litterarum a, b, c, d habebuntur, quos tam affirmative, quam negative accipere licet. Quodsi vero minores numeri pro A, B, C, D desiderentur, conveniet pro $aa+3bb$ et $3cc+dd$ ejusmodi valores capi, qui communem habeant divisorem. Statuatur ergo

$$aa+3bb=mk \quad \text{et} \quad dd+3cc=nk.$$

Tum vero sit $ac+bd=f$ et $3bc-ad=g$, hincque fiet:

$$\begin{aligned} A &= n(3f+g)-mmk, \\ B &= n(3f-g)+mmk, \\ C &= nnk-m(3f+g), \\ D &= nnk+m(3f-g), \end{aligned}$$

ubi notandum est, quicunque valores pro f et g fuerint inventi, eos tam affirmative, quam negative capi posse, ob numeros a, b, c, d ambiguos; unde pro quovis casu sequentes habebuntur determinationes:

$$\text{vel} \quad \begin{aligned} f &= \pm(ac+bd) \\ g &= \pm(3bc-ad) \end{aligned} \qquad \text{vel} \quad \begin{aligned} f &= \pm(ac-bd) \\ g &= \pm(3bc+ad). \end{aligned}$$

Patet autem, si manente g capiatur f negative, eosdem numeros esse prodituros ordine tantum permutato, unde sufficit pro f valores tantum affirmativos assumsisse. Praeterea manifestum est, si sit $m=n$, seu $aa+3bb=dd+3cc$, tum fore $A=-C$ et $D=B$, unde et hos casus excludi oportebit. Denique si $f=0$, fit $A=-B$ et $C=-D$; qui propterea casus quoque sunt omittendi. Saepenumero quoque evenit, ut vel pro a et b, vel pro c et d, vel pro utrisque plures valores oriantur, ex quibus solutionum numerus eo major evadit.

26. *Exempl.* 1. Capiatur $aa+3bb=19$, erit $a=4$ et $b=1$, tum vero $dd+3cc=76$, eritque

$$\text{vel} \quad \begin{aligned} d &= 1 \\ c &= 5 \end{aligned} \qquad \text{vel} \quad \begin{aligned} d &= 7 \\ c &= 3 \end{aligned} \qquad \text{vel} \quad \begin{aligned} d &= 8 \\ c &= 2. \end{aligned}$$

Tum vero fit $m=1$, $n=4$ et $k=19$. Pro f autem et g sequentes prodibunt valores:

$$\text{I.} \quad \begin{aligned} f &= 21, \\ g &= \pm 11, \end{aligned} \qquad \text{II.} \quad \begin{aligned} f &= 19, \\ g &= \pm 19, \end{aligned} \qquad \text{III.} \quad \begin{aligned} f &= 19, \\ g &= \pm 19, \end{aligned}$$

$$\text{IV.} \quad \begin{aligned} f &= 5, \\ g &= \pm 37, \end{aligned} \qquad \text{V.} \quad \begin{aligned} f &= 16, \\ g &= \pm 26, \end{aligned} \qquad \text{VI.} \quad \begin{aligned} f &= 0, \\ g &= \pm 38, \end{aligned}$$

unde tertius casus et sextus sunt excludendi. Atque hinc erit:

$$\begin{aligned} A &= 12f+4g-19, \\ B &= 12f-4g+19, \\ C &= 304-3f-g, \\ D &= 304+3f-g. \end{aligned}$$

Hinc ergo reperietur pro valore primo $f=21$ et $g=\pm 11$

		pro signis sup.	pro signis inf.		
I.	$A = 233 \pm 44$	$A = 277$	$A = 189$	seu	$A = 3$
	$B = 271 \mp 44$	$B = 227$	$B = 315$		$B = 5$
	$C = 241 \mp 11$	$C = 230$	$C = 252$		$C = 4$
	$D = 367 \mp 11$	$D = 356$	$D = 378$		$D = 6$

Casus autem II et III, dividendo formulas per 19, ob $f = 1.19$ et $g = \pm 1.19$, dabunt:

		vel			vel
$A = 11 \pm 4$	ergo	$A = 15$	seu	$A = 5$	$A = 7$
$B = 13 \mp 4$		$B = 9$		$B = 3$	$B = 17$
$C = 13 \mp 1$		$C = 12$		$C = 4$	$C = 14$
$D = 19 \mp 1$		$D = 18$		$D = 6$	$D = 20$

Casus IV, quo $f = 5$ et $g = \pm 37$, dat:

		vel			vel
$A = 41 \pm 148$	ergo	$A = 189$	seu	$A = 63$	$A = -107$
$B = 79 \mp 148$		$B = -69$		$B = -23$	$B = 227$
$C = 289 \mp 37$		$C = 252$		$C = 84$	$C = 326$
$D = 319 \mp 37$		$D = 282$		$D = 94$	$D = 356$

Casus V, quo $f = 16$ et $g = \pm 26$, dat:

$A = 173 \pm 104$	ergo	$A = 277$	$A = 69$	seu	$A = 23$
$B = 211 \mp 104$		$B = 107$	$B = 315$		$B = 105$
$C = 256 \mp 26$		$C = 230$	$C = 282$		$C = 94$
$D = 352 \mp 26$		$D = 326$	$D = 378$		$D = 126$

En ergo plures cuborum terniones ex unica positione inventos:

$227^3 + 230^3 + 277^3 = 356^3$	$107^3 + 356^3 = 227^3 + 326^3$
$107^3 + 230^3 + 277^3 = 326^3$	$23^3 + 94^3 = 63^3 + 84^3$
$23^3 + 94^3 + 105^3 = 126^3$	
$7^3 + 14^3 + 17^3 = 20^3$	
$3^3 + 4^3 + 5^3 = 6^3$	

unde colligitur

$$356^3 - 227^3 = 230^3 + 277^3 = 326^3 - 107^3, \quad \text{item}$$
$$126^3 - 105^3 = 63^3 + 84^3 = 23^3 + 94^3.$$

27. *Exempl.* 2. Sit $aa + 3bb = 28$, erit

$$\text{vel} \begin{cases} a = 1 \\ b = 3 \end{cases} \quad \text{vel} \begin{cases} a = 4 \\ b = 2 \end{cases} \quad \text{vel} \begin{cases} a = 5 \\ b = 1 \end{cases}$$

cum vero sit: $dd + 3ee = 84$, erit

$$\text{vel} \begin{cases} d = 3 \\ c = 5 \end{cases} \quad \text{vel} \begin{cases} d = 6 \\ c = 4 \end{cases} \quad \text{vel} \begin{cases} d = 9 \\ c = 1 \end{cases}$$

hincque $k = 28$, $m = 1$ et $n = 3$, tum vero pro f et g sequentes prodibunt valores:

$$\text{I.} \begin{array}{l} f = 14, \\ g = \pm 42, \end{array} \qquad \text{II.} \begin{array}{l} f = 4, \\ g = \pm 48, \end{array} \qquad \text{III.} \begin{array}{l} f = 22, \\ g = \pm 30, \end{array}$$

$$\text{IV.} \begin{array}{l} f = 14, \\ g = \pm 42, \end{array} \qquad \text{V.} \begin{array}{l} f = 28, \\ g = \pm 0, \end{array} \qquad \text{VI.} \begin{array}{l} f = 26, \\ g = \pm 18, \end{array}$$

ubi notandum est, hos valores, quorum I et IV conveniunt, oriri ex sola positione $a = 1$ et $b = 3$, et reliquas duas eosdem producere. Hinc ergo habebimus:

$$\begin{array}{l} A = 9f + 3g - 28 \\ B = 9f - 3g + 28 \\ C = 252 - 3f - g \\ \hline D = 252 + 3f - g \end{array}$$

unde casus primus et quartus dabunt per 14 dividendo

$$\begin{array}{l} A = 7 \pm 9 \\ B = 11 \mp 9 \\ C = 15 \mp 3 \\ \hline D = 21 \mp 3 \end{array} \quad \text{ergo I.} \begin{array}{l} A = 16 = 8 \\ B = 2 = 1 \\ C = 12 = 6 \\ \hline D = 18 = 9 \end{array} \quad \text{II.} \begin{array}{l} A = -2 = -1 \\ B = 20 = 10 \\ C = 18 = 9 \\ \hline D = 24 = 12 \end{array}$$

Casus vero secundus per 4 dividendo dat:

$$\begin{array}{l} A = 2 \pm 36 \\ B = 16 \mp 36 \\ C = 60 \mp 12 \\ \hline D = 66 \mp 12 \end{array} \quad \text{ergo I.} \begin{array}{l} A = 38 = 19 \\ B = -20 = -10 \\ C = 48 = 24 \\ \hline D = 54 = 27 \end{array} \quad \text{II.} \begin{array}{l} A = -34 = -17 \\ B = 52 = 26 \\ C = 72 = 36 \\ \hline D = 78 = 39 \end{array}$$

Casus tertius per 2 divisus dat:

$$\begin{array}{l} A = 85 \pm 45 \\ B = 113 \mp 45 \\ C = 93 \mp 15 \\ \hline D = 159 \mp 15 \end{array} \quad \text{ergo I.} \begin{array}{l} A = 130 = 65 \\ B = 68 = 34 \\ C = 78 = 39 \\ \hline D = 144 = 72 \end{array} \quad \text{II.} \begin{array}{l} A = 40 = 20 \\ B = 158 = 79 \\ C = 108 = 54 \\ \hline D = 174 = 87 \end{array}$$

Casus quintus dat per 28 divisus:

$$\begin{array}{l} A = 8 = 4 \\ B = 10 = 5 \\ C = 6 = 3 \\ \hline D = 12 = 6 \end{array}$$

Casus denique sextus per 2 divisus, dat:

$$\begin{array}{l} A = 103 \pm 27 \\ B = 131 \mp 27 \\ C = 87 \mp 9 \\ \hline D = 165 \mp 9 \end{array} \quad \text{ergo vel} \quad \begin{array}{l} A = 130 = 65 = 5 \\ B = 104 = 52 = 4 \\ C = 78 = 39 = 3 \\ \hline D = 156 = 78 = 6 \end{array} \quad \text{vel} \quad \begin{array}{l} A = 76 = 38 \\ B = 158 = 79 \\ C = 96 = 48 \\ \hline D = 174 = 87 \end{array}$$

Ex hoc ergo exemplo sequentes resultant formulae:

$$\begin{array}{rl} 1^3 + 6^3 + 8^3 = 9^3 & \\ 34^3 + 39^3 + 65^3 = 72^3 & \qquad 1^3 + 12^3 = 9^3 + 10^3 \\ 20^3 + 54^3 + 79^3 = 87^3 & \text{ et } \quad 10^3 + 27^3 = 19^3 + 24^3 \\ 3^3 + 4^3 + 5^3 = 6^3 & \qquad 17^3 + 39^3 = 26^3 + 36^3 \\ 38^3 + 48^3 + 79^3 = 87^3 & \end{array}$$

hincque sequitur

$$87^3 - 79^3 = 20^3 + 54^3 = 38^3 + 48^3.$$

Patet ergo, ex quovis exemplo assumto plures hujusmodi formulas obtineri, inter quas autem eaedem saepius recurrent; quemadmodum casus $3^3 + 4^3 + 5^3 = 6^3$ in hoc exemplo et praecedente bis occurrit.

28. En ergo solutionem generalem problematis, quo quaeruntur quatuor numeri rationales A, B, C, D, ita ut sit $A^3 + B^3 + C^3 = D^3$, seu quod eodem redit, quo quaeruntur quatuor numeri rationales, p, q, r et s, ut sit $p(pp + 3qq) = s(ss + 3rr)$. Quae problemata cum methodis solitis non nisi particulariter resolvi queant, manifestum est, has methodos solitas adhuc insigni defectu laborare, ideoque notabilem adhuc perfectionem desiderare. Tum vero, quod hic de unico problemate ostendimus, nullum est dubium, quin id in infinitis aliis pari successu praestari possit. In genere quidem patet, simili modo hujusmodi aequationem $\alpha p(mpp + nqq) = \beta s(mss + nrr)$, vel etiam hanc latius patentem

$$(\alpha p + \beta q + \gamma r + \delta s + \varepsilon)(mpp + nqq) = (ap + bq + cr + ds + e)(mrr + nss)$$

rationaliter generalissime resolvi posse, ponendo:

$$\begin{array}{l} p = nfx + gy \\ q = mfy - gx \end{array} \quad \text{et} \quad \begin{array}{l} r = nhx + ky \\ s = mhy - kx \end{array}$$

fiet enim

$$\begin{array}{l} mpp + nqq = (gg + mnff)(nxx + myy) \\ mrr + nss = (kk + mnhh)(nxx + myy) \end{array}$$

unde aequatio divisa per $nxx + myy$ continebit incognitas x et y unius tantum dimensionis, ex qua propterea sine ulla restrictione earum valores rationaliter determinabuntur.

29. Non immerito igitur suspicari licet, et aliorum problematum Diophanteorum, quorum adhuc non nisi solutiones particulares sunt repertae, solutiones quoque generales dari, neque discrimen supra memoratum, ex solutionum generalitate et particularitate petitum, esse essentiale; unde patet quanta adhuc incrementa in analysi Diophantea desiderentur. Ad quae si unquam penetrare contigerit, nullum est dubium, quin inde universa analysis, tam finitorum, quam infinitorum, haud

contemnenda subsidia sit acceptura. Cum enim in calculo integrali praecipuum artificium in hoc versetur, ut formulae differentiales irrationales in rationales transformentur: hoc artificium ipsum, uti ex analysi Diophantea in hunc calculum est translatum, ita etiam indidem majora auxilia merito expectantur; ex quo studium, quod in ista analysi, utcunque sterilis alias in se spectata videatur, amplificanda impenditur, neutiquam inutiliter collocari est censendum.

30. Hic porro alia conditio non minus attentione digna notari meretur, quod saepius in analysi Diophantea ejusmodi problemata occurrunt, quae per methodos consuetas solutionem generalem admittere videntur, cum tamen haec solutio tantum sit particularis; quibus casibus peculiaria artificia adhiberi debent, ut restrictio, qua methodus consueta est limitata, tollatur. Veluti si duo cubi in numeris integris quaerantur, quorum summa sit numerus quadratus; solutio nullo modo restricta obtineri videtur, si ista aequatio $x^3+y^3=zz$ ita resolvatur, ut ponatur $x=\frac{pz}{r}$ et $y=\frac{qz}{r}$. Fiet enim $(p^3+q^3)z=r^3$, ideoque $z=\frac{r^3}{p^3+q^3}$, et $x=\frac{prr}{p^3+q^3}$, $y=\frac{qrr}{p^3+q^3}$. Unde, ut x et y fiant numeri integri, statuatur $r=n(p^3+q^3)$, ut habeatur:

$$x=nnp(p^3+q^3) \quad \text{et} \quad y=nnq(p^3+q^3)$$

eritque $x^3+y^3=n^6(p^3+q^3)^4=$ quadrato.

31. Etsi autem ista solutio generalis videtur, tamen nulli alii numeri pro x et y inveniuntur, nisi qui communem habent factorem p^3+q^3, ita ut hinc concludendum videatur, nullos dari numeros inter se primos, qui, pro x et y substituti, quaestioni satisfaciant. Interim tamen casu, quo $x=1$ et $y=2$, perspicuum est, fore $x^3+y^3=9=$ quadrato. Tametsi autem hic casus ex formulis nostris derivari potest, ponendo $p=1$, $q=2$, et $n=\frac{1}{3}$, unde utique prodit $x=\frac{1}{9}.9=1$ et $y=\frac{2}{9}.9=2$; tamen ut hinc alii hujus generis casus eliciantur, necesse est, ut pro p et q ejusmodi numeri accipiantur, quorum cuborum summa sit quadratum, puta $=ss$, ut deinceps poni possit $n=\frac{1}{s}$: unde prodibit $x=p$ et $y=q$: quo pacto id ipsum, quod hic quaeritur, jam tanquam cognitum postulatur, ut scilicet duo cubi assignari queant, quorum summa sit quadratum. Quemadmodum ergo huic incommodo sit occurrendum, in sequenti problemate videamus.

32. **Problema.** Invenire duos numeros integros inter se primos, quorum cubi additi faciant quadratum.

Solutio. Sint x et y numeri quaesiti, ita ut esse debeat $x^3+y^3=$ quadrato. Debet ergo $(x+y)(xx-xy+yy)$ esse $=$ quadrato. At de his duobus factoribus annoto, eos esse vel primos inter se, vel ternarium pro communi mensura admittere, unde solutio fiet bipartita, qua autem ita in unam compingetur, ut uterque factor seorsim, $x+y$ et $xx-xy+yy$, vel quadratum esse debeat, vel triplum quadratum.

I. Sit primum uterque factor quadratus; ac ponatur $xx-xy+yy=(pp-pq+qq)^2$, eritque vel $x=pp-2pq$ et $y=pp-qq$, vel $x=2pq-pp$ et $y=qq-pp$. Priori casu ergo oportet ut sit $x+y=2pp-2pq-qq$ quadratum. Quae forma cum sit $=3pp-(p+q)^2$, si ponatur $=rr$, oporteret esse $3pp=(p+q)^2+rr=$ summae duorum quadratorum, quod est

impossibile. Relinquitur ergo alter casus, quo $x + y = qq + 2pq - 2pp = (q + p)^2 - 3pp =$ quadrato, cui satisfit ponendo

$$p = 2mn \quad \text{et} \quad q = 3mm - 2mn + nn,$$
$$x = 2pq - pp = 4mn(3mm - 3mn + nn),$$
$$y = qq - pp = (3mm + nn)(3mm - 4mn + nn) = (m - n)(3m - n)(3mm + nn).$$

II. Tum vero ponatur $xx - xy + yy =$ triplo quadrato $= 3(pp - pq + qq)^2$, cui triplici modo satisfit:

I. $x = 2pp - 2pq - qq$, $y = pp + 2pq - 2qq$ II. $x = 2pp - 2pq - qq$, $y = pp - 4pq + qq$ III. $x = pp + 2pq - 2qq$, $y = -pp + 4pq - qq$.

Casu primo fit:

$x + y = 3pp - 3qq =$ triplo quadrato, seu $pp - qq =$ quadrato: unde fit $p = mm + nn$ et $q = 2mn$, ideoque

$$x = 2(m^4 - 2m^3n - 2mn^3 + n^4),$$
$$y = m^4 + 4m^3n - 6mmnn + 4mn^3 + n^4.$$

Casu secundo fit:

$x + y = 3pp - 6pq =$ triplo quadrato; ergo $pp - 2pq =$ quadrato, cui satisfit ponendo $p = 2mm$ et $q = mm - nn$; unde oritur

$$x = 3m^4 + 6mmnn - n^4,$$
$$y = -3m^4 + 6mmnn + n^4.$$

Casu denique tertio fit:

$$x + y = 6pq - 3qq = 3\square \text{ et } 2pq - qq = \square$$

unde fit: $p = mm + nn$ et $q = 2mm$; ideoque

$$x = -3m^4 + 6mmnn + n^4,$$
$$y = 3m^4 + 6mmnn - n^4,$$

quae cum illis congruunt.

En ergo ternas solutiones problematis propositi:

$$\text{I.} \begin{cases} x = 4mn(3mm - 3mn + nn) \\ y = (m - n)(3m - n)(3mm + nn \end{cases}$$

$$\text{II.} \begin{cases} x = 2(m^4 - 2m^3n - 2mn^3 + n^4) \\ y = m^4 + 4m^3n - 6mmnn + 4mn^3 + n^4 \end{cases}$$

$$\text{III.} \begin{cases} x = 3m^4 + 6mmnn - n^4 \\ y = -3m^4 + 6mmnn + n^4 \end{cases}$$

ubi quidem secunda forma in tertia, quae cum quarta convenit, contenta deprehenditur, ita ut secunda, uti magis complicata, omitti possit.

33. **Coroll. 1.** Si hae formulae, pro x et y inventae, per numerum quadratum quemcunque multiplicentur, eae quaesito aeque satisfacient, ita scilicet summa cuborum x^3+y^3 fiat numerus quadratus, unde numeri quotcunque non primi inter se obtinebuntur. Simili autem modo si hae formulae communem habuerint divisorem quadratum, per eum divisae quaesito perinde satisfacient, unde numeri inter se primi pro x et y inveniuntur, quales hic proprie quaeruntur. Geminas ergo pro hoc negotio habebimus formulas:

I. $x = 4mn(3mm - 3mn + nn)$
$y = (m-n)(3m-n)(3mm+nn)$

II. $x = 3m^4 + 6mmnn - n^4$
$y = -3m^4 + 6mmnn + n^4$.

34. **Coroll. 2.** Evidens est, dari infinitos casus, quibus altera harum formularum recipit valorem negativum: quod in prioribus evenit, si vel m sit negativum, vel n; vel n contineatur intra limites m et $3m$: in posterioribus autem, si vel $\frac{nn}{mm}$ sit majus, quam $3(1+\sqrt{2})$, vel $\frac{nn}{mm}$ minus, quam $3(\sqrt{2}-1)$. His ergo casibus duo reperiuntur cubi, quorum differentia est quadratum.

XV.

Demonstratio theorematis Fermatiani, omnem numerum primum formae $4n+1$ esse summam duorum quadratorum. (*)

(N. Comment. V. 1754 — 55. p. 3.)

§ 1. Cum nuper eos essem contemplatus numeros, qui ex additione duorum quadratorum oriuntur, plures demonstravi proprietates, quibus tales numeri sunt praediti (**): neque tamen meas meditationes eo usque perducere licuit, ut hujus theorematis, quod Fermatius olim geometris demonstrandum proposuit, veritatem solide ostendere potuissem. Tentamen tamen demonstrationis tum exposui (l. c. pag. 163. § 28), unde certitudo hujus theorematis multo luculentius elucet, etiamsi criteriis rigidae demonstrationis destituatur: neque dubitavi, quin iisdem vestigiis insistendo tandem demonstratio desiderata facilius obtineri possit; quod quidem ex eo tempore mihi ipsi usu venit, ita, ut tentamen illud, si alia quaedam levis consideratio accedat, in rigidam demonstrationem abeat. Nihil quidem novi in hac re me praestitisse gloriari possum, cum ipse Fermatius jam demonstrationem hujus theorematis elicuisse se profiteatur; verum, quod eam nusquam publici juris fecit, ejus jactura perinde ac plurimorum aliorum egregiorum hujus viri inventorum efficit, ut, quae nunc demum de his deperditis rebus quasi recuperamus, ea non immerito pro novis inventis habeantur. Cum enim nemo unquam tam feliciter in arcana numerorum penetraverit, quam Fermatius, omnis opera in hac scientia ulterius excolenda frustra impendi videtur, nisi ante, quae ab hoc excellenti viro jam fuerunt investigata, quasi de novo in lucem protrahantur. Etsi enim post eum plures viri docti in hoc studiorum genere vires suas exercuerunt, nihil tamen plerumque sunt consecuti, quod cum ingenio hujus viri comparari posset.

§ 2. Ut autem demonstrationem theorematis, quod hic considero, instituam, duas propositiones in subsidium vocari oportet, quarum demonstrationem jam alibi dedi. Altera est, quod omnes numeri, qui sunt divisores summae duorum quadratorum inter se primorum, ipsi sint summae duorum quadratorum, sic si a et b sint numeri inter se primi, atque numeri ex iis formati $aa+bb$ divisor sit d, erit quoque d summa duorum quadratorum: hujus theorematis demonstrationem dedi in scripto ante memorato, quo numeros, qui sunt duorum quadratorum summae, sum contemplatus (l. c. pag. 161. § 22). Altera propositio, qua demonstratio sequens indiget, ita se habet: si p sit numerus primus, atque a et b numeri quicunque per p non divisibiles, erit semper $a^{p-1}-b^{p-1}$ per numerum primum p divisibilis: demonstrationem hujus rei jam dudum in Nov. Comment. Acad. Petrop. Tom. I dedi (***).

§ 3. Quodsi jam $4n+1$ sit numerus primus, per eum omnes numeri in hac forma $a^{4n}-b^{4n}$ contenti erunt divisibiles, siquidem neuter numerorum a et b seorsim per $4n+1$ fuerit divisibilis.

(*) Haecce omnino est commentatio, ad quam citationem pag. 174 referri oportet (vide § 97 et seqq.). Ea igitur non solum ante dissertationem XIII Commentariis fuit inserta, sed quoque prius videtur exhibita. Ipsum vero exhibitionis diem nobis exacte eruere non licuit. (**) Vide comment. XII. pag. 155 sqq. (***) Vide hujus operis comment. VII. pag. 52.

Quare si a et b sint numeri minores, quam $4n+1$, (cyphra tamen excepta), numerus inde formatus $a^{4n}-b^{4n}$ sine ulla limitatione per numerum primum propositum $4n+1$ erit divisibilis. Cum autem $a^{4n}-b^{4n}$ sit productum horum factorum $a^{2n}+b^{2n}$ et $a^{2n}-b^{2n}$, necesse est, ut alteruter horum factorum sit per $4n+1$ divisibilis; fieri enim nequit, ut vel neuter, vel uterque simul divisorem habeat $4n+1$. Quodsi jam demonstrari posset, dari casus, quibus forma $a^{2n}+b^{2n}$ sit divisibilis per $4n+1$, quoniam $a^{2n}+b^{2n}$, ob exponentem $2n$ parem, est summa duorum quadratorum, quorum neutrum seorsim per $4n+1$ divisibile existit, inde sequeretur, hunc numerum $4n+1$ esse summam duorum quadratorum.

§ 4. Verum summa $a^{2n}+b^{2n}$ toties erit per $4n+1$ divisibilis, quoties differentia $a^{2n}-b^{2n}$ per eundem numerum non est divisibilis. Quare qui negaverit, numerum primum $4n+1$ esse summam duorum quadratorum, is negare cogitur, ullum numerum hujus formae $a^{2n}+b^{2n}$ per $4n+1$ esse divisibilem: eundem propterea affirmare oportet, omnes numeros in hac forma $a^{2n}-b^{2n}$ contentos per $4n+1$ esse divisibiles; siquidem neque a, neque b per $4n+1$ sit divisibile. Quamobrem mihi hic demonstrandum est, non omnes numeros in forma $a^{2n}-b^{2n}$ contentos per $4n+1$ esse divisibiles; hoc enim si praestitero, certum erit, dari casus, seu numeros pro a et b substituendos, quibus forma $a^{2n}-b^{2n}$ non sit per $4n+1$ divisibilis; illis ergo casibus altera forma $a^{2n}+b^{2n}$ necessario per $4n+1$ erit divisibilis: unde cum a^{2n} et b^{2n} sint numeri quadrati, conficietur id, quod proponitur, scilicet numerum $4n+1$ esse summam duorum quadratorum.

§ 5. Ut igitur demonstrem, non omnes numeros in hac forma $a^{2n}-b^{2n}$ contentos, seu non omnes differentias inter binas potestates dignitatis $2n$ esse per $4n+1$ divisibiles, considerabo seriem harum potestatum ab unitate usque ad eam, quae a radice $4n$ formatur:

$$1,\ 2^{2n},\ 3^{2n},\ 4^{2n},\ 5^{2n},\ 6^{2n}\ \ldots\ldots\ (4n)^{2n}$$

ac jam dico, non omnes differentias inter binos terminos hujus seriei esse per $4n+1$ divisibiles. Si enim singulae differentiae primae

$$2^{2n}-1,\ 3^{2n}-2^{2n},\ 4^{2n}-3^{2n},\ 5^{2n}-4^{2n},\ \ldots\ldots\ (4n)^{2n}-(4n-1)^{2n}$$

per $4n+1$ essent divisibiles, etiam differentiae hujus progressionis, quae sunt differentiae secundae illius seriei, per $4n+1$ essent divisibiles: atque ob eandem rationem differentiae tertiae, quartae, quintae, etc. omnes forent per $4n+1$ divisibiles; ac denique etiam differentiae ordinis $2n$, quae sunt, ut constat, omnes inter se aequales. Differentiae autem ordinis $2n$ sunt $=1.\,2.\,3.\,4\ldots\ldots 2n$, quae ergo per numerum primum $4n+1$ non sunt divisibiles, ex quo vicissim sequitur, ne omnes quidem differentias primas per $4n+1$ esse divisibiles.

§ 6. Quo vis hujus demonstrationis melius perspiciatur, notandum est, differentiam ordinis $2n$ produci ex $2n+1$ terminis seriei propositae, qui si ab initio capiantur, omnes ita sunt comparati, ut binorum quorumvis differentiae per $4n+1$ divisibiles esse debeant, si theorematis veritas negetur. Sin autem plures termini ad hanc differentiam ultimam constituendam concurrerent, iique ultra terminum $(4n)^{2n}$ progrederentur, quoniam differentiae a termino sequente $(4n+1)^{2n}$ ortae ad enunciata theorematis non pertinent, demonstratio nullam vim retineret. Hinc autem, quod differentia ultima, quam sumus contemplati, tantum ab $2n+1$ terminis pendet, conclusio, quam inde de-

duximus, omnino est legitima; indeque sequitur, dari differentias primas, veluti $a^{2n}-(a-1)^{2n}$, quae non sint per $4n+1$ divisibiles, atque ita quidem, ut a non sit major, quam $2n+1$. Hinc autem porro recte infertur, summam $a^{2n}+(a-1)^{2n}$, ideoque summam duorum quadratorum per $4n+1$ necessario esse divisibilem: ideoque numerum primum $4n+1$ summam esse duorum quadratorum.

§ 7. Quoniam differentia ordinis $2n$ ab $2n+1$ terminis seriei potestatum pendet, totidem tantum ab initio captos consideremus

$$1,\ 2^{2n},\ 3^{2n},\ 4^{2n},\ 5^{2n},\ 6^{2n}\ \ldots\ldots\ (2n)^{2n},\ (2n+1)^{2n}$$

unde differentiae primae erunt:

$$2^{2n}-1,\ 3^{2n}-2^{2n},\ 4^{2n}-3^{2n},\ 5^{2n}-4^{2n},\ \ldots\ldots\ (2n+1)^{2n}-(2n)^{2n},$$

cujus progressionis terminorum numerus est $=2n$. Ex demonstratione itaque praecedente patet, non omnes terminos hujus progressionis differentiarum esse per numerum primum $4n+1$ divisibiles; neque tamen hinc intelligimus, quot et quinam sint illi termini, per $4n+1$ non divisibiles. Ad demonstrationem enim sufficit, si vel unicus terminus, quisquis ille fit, per $4n+1$ non sit divisibilis. Quodsi autem casus speciales evolvamus, quibus $4n+1$ est numerus primus, ex differentiis istis, quarum numerus est $=2n$, reperiemus, semper semissem esse per $4n+1$ divisibilem, alterum vero semissem non divisibilem: quae observatio etsi ad vim demonstrationis non spectat, tamen ad eam illustrandam non parum confert, quare aliquot casus speciales ad examen revocasse juvabit.

§ 8. Minimus numerus primus formae $4n+1$ est $=5$, qui oritur, si $n=1$; unde duae habebuntur differentiae 2^2-1 et 3^2-2^2, quarum prior non est divisibilis per 5, altera vero est divisibilis. Pro reliquis casibus utamur signo d ad eas differentias indicandas, quae sunt divisibiles, at signo 0 eas notemus, quae non sunt divisibiles, quae signa differentiis pro quovis casu subscribamus

$4n+1$	Differentiae							
13	2^6-1,	3^6-2^6,	4^6-3^6,	5^6-4^6,	6^6-5^6,	7^6-6^6:		
	0	0	d	0	d	d		
17	2^8-1,	3^8-2^8,	4^8-3^8,	5^8-4^8,	6^8-5^8,	7^8-6^8,	8^8-7^8,	9^8-8^8
	d	0	0	0	d	d	0	d
29	$2^{14}-1$,	$3^{14}-2^{14}$,	$4^{14}-3^{14}$,	$5^{14}-4^{14}$,	$6^{14}-5^{14}$,	$7^{14}-6^{14}$,	$8^{14}-7^{14}$,	$9^{14}-8^{14}$,
	0	d	0	d	d	d	0	0
	$10^{14}-9^{14}$,	$11^{14}-10^{14}$,	$12^{14}-11^{14}$,	$13^{14}-12^{14}$,	$14^{14}-13^{14}$,	$15^{14}-14^{14}$		
	0	d	d	0	0	d		

Hinc patet, terminos divisibiles et non divisibiles nulla certa lege contineri, etiamsi utrique sint multitudine pares: tamen per se est perspicuum, ultimum terminum $(2n+1)^{2n}-(2n)^{2n}$ semper per $4n+1$ esse divisibilem, quia factorem habet $(2n+1)^2-4nn=4n+1$: at de reliquis nihil certi statui potest.

§ 9. Porro quoque ad vim demonstrationis penitius perspiciendam notari oportet, demonstrationem tum solum locum habere, si numerus $4n+1$ sit primus; prorsus uti natura theorematis postulat. Nam si $4n+1$ non esset numerus primus, neque de eo affirmari posset, quod sit summa duorum quadratorum, neque forma $a^{4n}-b^{4n}$ per eum esset necessario divisibilis. Quin etiam ultima conclusio foret falsa, qua pronunciavimus, differentias illas ordinis $2n$, quae sunt $=1.2.3.4\ldots 2n$, non esse per $4n+1$ divisibiles. Si enim $4n+1$ non esset numerus primus, sed factores haberet, qui essent minores, quam $2n$, tum utique productum $1.2.3.4\ldots 2n$ hos factores contineret, foretque idcirco per $4n+1$ divisibile. At si $4n+1$ est numerus primus, tum demum affirmare licet, productum $1.2.3.4\ldots 2n$ plane non esse per $4n+1$ divisibile: quia hoc productum per nullos alios numeros dividi potest, nisi qui tanquam factores in illud ingrediuntur.

§ 10. Cum denique demonstratio tradita hoc nitatur fundamento, quod seriei potestatum $1,\ 2^{2n},\ 3^{2n},\ 4^{2n}$, etc. differentiae ordinis $2n$ sint constantes, omnesque $=1.2.3.4\ldots\ldots 2n$, hoc uberius explicandum videtur, etsi passim in libris analyticorum solide expositum reperitur. Primum igitur notandum est, si seriei cujuscunque terminus generalis, seu is qui exponenti indefinito x respondet, sit

$$=Ax^m+Bx^{m-1}+Cx^{m-2}+Dx^{m-3}+Ex^{m-4}+\text{etc.}$$

hanc seriem ad gradum m referri, quia m est exponens maximae potestatis ipsius x. Deinde si hic terminus generalis a sequente

$$A(x+1)^m+B(x+1)^{m-1}+C(x+1)^{m-2}+\text{etc.}$$

subtrahatur, prodibit terminus generalis seriei differentiarum, in quo exponens summae potestatis ipsius x erit $=m-1$, ideoque series differentiarum ad gradum inferiorem $m-1$ pertinebit. Pari modo ex termino generali seriei differentiarum primarum colligetur terminus generalis seriei differentiarum secundarum, qui igitur denuo ad gradum depressiorem $m-2$ pertinebit.

§ 11. Ita si series proposita ad gradum m referatur, series differentiarum primarum, ad gradum $m-1$ referetur; series porro differentiarum secundarum ad gradum $m-2$; series differentiarum tertiarum ad gradum $m-3$; series differentiarum quartarum ad gradum $m-4$; et in genere series differentiarum ordinis n ad gradum $m-n$ pertinebit. Unde series differentiarum ordinis m ad gradum $m-m=0$ perveniet, ejusque ergo terminus generalis, quia summa ipsius x potestas est $=x^0=1$, erit quantitas constans, ideoque omnes differentiae ordinis m inter se erunt aequales. Hinc serierum primi gradus, quarum terminus generalis est $=Ax+B$, jam differentiae primae sunt inter se aequales: serierum autem secundi gradus, quae hoc termino generali Ax^2+Bx+C continentur, differentiae secundae sunt aequales, et ita porro.

§ 12. Quodsi ergo seriem quamcunque potestatum consideremus

$$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m,\ 6^m,\ 7^m,\ 8^m,\ \text{etc.}$$

cujus terminus generalis est $=x^m$, seu is, qui indici x respondet, series differentiarum ordinis m ex terminis inter se aequalibus constabit. At seriei differentiarum primarum terminus generalis erit $=(x+1)^m-x^m$; qui a sequente $(x+2)^m-(x+1)^m$ subtractus dabit terminum generalem seriei differentiarum secundarum, qui erit

$$=(x+2)^m-2(x+1)^m+x^m.$$

Hinc porro seriei differentiarum tertiarum erit terminus generalis

$$= (x+3)^m - 3(x+2)^m + 3(x+1)^m - x^m;$$

ac tandem seriei differentiarum ordinis m concluditur terminus generalis

$$= (x+m)^m - m(x+m-1)^m + \frac{m(m-1)}{1.\,2}(x+m-2)^m - \frac{m(m-1)(m-2)}{1.\,2.\,3}(x+m-3)^m + \text{etc.},$$

qui cum sit quantitas constans, idem erit quicunque numerus pro x substituatur, erit ergo

$$\text{vel } = m^m - m(m-1)^m + \frac{m(m-1)}{1.\,2}(m-2)^m - \frac{m(m-1)(m-2)}{1.\,2.\,3}(m-3)^m + \text{etc.},$$

$$\text{vel } = (m+1)^m - m.m^m + \frac{m(m-1)}{1.\,2}(m-1)^m - \frac{m(m-1)(m-2)}{1.\,2.\,3}(m-2)^m + \text{etc.},$$

ubi in forma priori posuimus $x = 0$, in posteriori $x = 1$.

§ 13. Evolvamus jam casus hujus seriei speciales et a potestatibus minimis ad altiores ascendamus: ac posito primo $m = 1$, seriei 1, 2, 3, 4, 5, 6, etc. terminus generalis differentiarum primarum erit $= 1^1 - 1.\,0^1 = 1$, vel $= 2^1 - 1.\,1^1 = 1$. Si $m = 2$, seriei 1, 2^2, 3^2, 4^2, 5^2, etc. differentiae secundae sunt vel $2^2 - 2.\,1^2$, vel $3^2 - 2.\,2^2 + 1.\,1^2$; at est $2^2 - 2.\,1^2 = 2(2^1 - 1.\,1^1)$, unde haec differentiae secundae sunt $= 2.\,1$. Sit $m = 3$, et seriei 1, 2^3, 3^3, 4^3, 5^3, etc. differentiae tertiae erunt vel $= 3^3 - 3.\,2^3 + 3.\,1^3$, vel $4^3 - 3.\,3^3 + 3.\,2^3 - 1.\,1^3$, at

$$3^3 - 3.\,2^3 + 3.\,1^3 = 3(3^2 - 2.\,2^2 + 1.\,1^2) = 3.\,2.\,1,$$

quia ex casu praecedente est $3^2 - 2.\,2^2 + 1.\,1^2 = 2.\,1$. Simili modo si $m = 4$ seriei 1, 2^4, 3^4, 4^4, 5^4, etc. differentiae quartae erunt

$$\text{vel } 4^4 - 4.\,3^4 + 6.\,2^4 - 4.\,1^4, \quad \text{vel } 5^4 - 4.\,4^4 + 6.\,3^4 - 4.\,2^4 + 1.\,1^4.$$

At est

$$4^4 - 4.\,3^4 + 6.\,2^4 - 4.\,1^4 = 4(4^3 - 3.\,3^3 + 3.\,2^3 - 1.\,1^3) = 4.\,3.\,2.\,1.$$

§ 14. Quo hic progressus melius perspiciatur, sint seriei 1, 2^m, 3^m, 4^m, 5^m, etc. differentiae ordinis $m = P$; seriei 1, 2^{m+1}, 3^{m+1}, 4^{m+1}, 5^{m+1} etc. differentiae ordinis $m + 1 = Q$, erit

$$P = (m+1)^m - m.m^m + \frac{m(m-1)}{1.\,2}(m-1)^m - \frac{m(m-1)(m-2)}{1.\,2.\,3}(m-2)^m + \text{etc.}$$

$$Q = (m+1)^{m+1} - (m+1)m^{m+1} + \frac{(m+1)m}{1.\,2}(m-1)^{m+1} - \frac{(m+1)m(m-1)}{1.\,2.\,3}(m-2)^{m+1} + \text{etc.}$$

Ubi P ex forma posteriori, at Q ex forma priori expressimus. Hic primo patet, in utraque expressione parem esse terminorum numerum, et singulos terminos expressionis P esse ad singulos terminos expressionis Q, uti 1 ad $m + 1$. Namque est

$$(m+1)^m : (m+1)^{m+1} = 1 : m+1,$$

$$m.m^m : (m+1)m^{m+1} = 1 : m+1,$$

$$\frac{m(m-1)}{1.\,2}(m-1)^m : \frac{(m+1)m}{1.\,2}(m-1)^{m+1} = 1 : m+1,$$

$$\frac{m(m-1)(m-2)}{1.\,2.\,3}(m-2)^m : \frac{(m+1)m(m-1)}{1.\,2.\,3}(m-2)^{m+1} = 1 : m+1,$$

etc.

Hanc ob rem erit $P : Q = 1 : m+1$, ideoque $Q = (m+1)P$.

§ 15. Hinc ergo patet fore

seriei	differentias
$1,\ 2,\ 3,\ 4,\ 5,$ etc.	primas $= 1$
$1,\ 2^2,\ 3^2,\ 4^2,\ 5^2,$ etc.	secundas $= 1.2.$
$1,\ 2^3,\ 3^3,\ 4^3,\ 5^3,$ etc.	tertias $= 1.2.3$
$1,\ 2^4,\ 3^4,\ 4^4,\ 5^4,$ etc.	quartas $= 1.2.3.4$
$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m,$ etc.	ordinis $m = 1.2.3\ldots m$

ergo

$1,\ 2^{2n},\ 3^{2n},\ 4^{2n},\ 5^{2n},$ etc.	ordinis $2n = 1.2.3\ldots 2n.$

Atque ita quoque demonstravimus, seriei potestatum $1,\ 2^{2n},\ 3^{2n},\ 4^{2n},\ 5^{2n}$, etc. differentias ordinis $2n$ non solum esse constantes, sed etiam aequari producto $1.2.3.\ldots 2n$, uti in demonstratione theorematis propositi assumsimus.

1. **Theorema 1.** Ex serie quadratorum 1, 4, 9, 16, 25, etc. nulli numeri per numerum primum p sunt divisibiles, nisi quorum radices sunt per eundem numerum p divisibiles.

Demonstratio. Si enim quispiam numerus quadratus aa fuerit per numerum primum p divisibilis, quia ex factoribus a et a constat, necesse est, ut alteruter factor per p sit divisibilis, quare numerus quadratus aa per numerum primum p divisibilis esse nequit, nisi ejus radix a sit divisibilis per p.

2. **Coroll. 1.** Numeri ergo quadrati per numerum primum p divisibiles nascuntur ex radicibus p, $2p$, $3p$, $4p$, etc. suntque ergo pp, $4pp$, $9pp$, $16pp$, etc. et reliqui numeri quadrati omnes per numerum primum p non erunt divisibiles.

3. **Coroll. 2.** Si ergo numeri quadrati, quorum radices in hac progressione arithmetica p, $2p$, $3p$, $4p$, etc. non continentur, per numerum primum p dividantur, in divisione semper residuum remanebit, quod erit minus, quam numerus p.

4. **Scholion.** Cujusmodi sint haec residua, quae ex divisione singulorum quadratorum per numerum primum quemcunque p nascuntur, in hac dissertatione diligentius investigare constitui. Plurima enim hic insignia phaenomena occurrent, quorum consideratione natura numerorum non mediocriter illustratur. Tam eximia autem in doctrina numerorum adhuc latent mysteria, in quibus evolvendis opera non frustra impendi videtur.

5. **Theorema 2.** Si series quadratorum in infinitum continuata in membra dispescatur, quorum singula ex p terminis constent, hoc modo

$$1,\ 4,\ldots pp \,|\, (p+1)^2 \ldots 4pp \,|\, (2p+1)^2 \ldots 9pp \,|\, (3p+1)^2 \ldots 16pp \,|\ \text{etc.}$$

tum si uniuscujusque membri termini singuli per numerum primum p dividantur, eadem residua eodemque ordine recurrent.

Demonstratio. Singulorum enim membrorum termini primi 1, $(p+1)^2$, $(2p+1)^2$, $(3p+1)^2$, etc. si per p dividantur, idem dabunt residuum $= 1$. Similique modo termini secundi 4, $(p+2)^2$, $(2p+2)^2$, $(3p+2)^2$ etc. per p divisi aequalia producent residua $= 4$, si quidem sit

$p > 4$. Eodemque modo patet, terminos tertios aequalia praebere residua, itemque quartos et quintos etc. Atque in genere, si primi membri terminus quotuscunque sit nn, reliquorum membrorum termini analogi erunt $(p+n)^2$, $(2p+n)^2$, $(3p+n)^2$ etc. qui omnes per p divisi idem relinquunt residuum, quod terminus nn. In singulis ergo membris eadem redeunt residua eodemque ordine.

6. **Coroll. 1.** Si igitur noverimus residua, quae ex terminis primi membri nascuntur, simul habebimus residua, quae ex divisione omnium reliquorum membrorum per numerum p facta oriuntur.

7. **Coroll. 2.** Quia postremus cujusque membri terminus per numerum p divisibilis existit, residuum erit $=0$; quemadmodum primi cujusque membri termini residuum est $=1$. Secundorum vero terminorum cujusque membri residuum erit $=4$, et tertiorum $=9$, quartorum $=16$ etc., si quidem sit $p > 4$, et $p > 9$, et $p > 16$ etc.

8. **Coroll. 3.** Quamdiu enim numeri quadrati 1, 4, 9, 16 etc. minores sunt, quam numerus p, illi ipsi residua constituent. Ex sequentibus vero quadratis numero p majoribus residua emergent alia ipso numero p minora.

9. **Scholion.** Ex divisionis natura constat, residua semper esse minora divisore p; ac si forte per inadvertentiam residuum relinquatur majus, quam divisor p, id subtrahendo p, quoties fieri potest, ad numerum ipso p minorem reducetur. Sic residuum $p+a$, et in genere $np+a$, quod forte ex divisione per p prodierit, aequivalebit residuo a; atque cum de residuis, quae ex divisione numerorum per p nascuntur, agitur, omnia haec residua a, $p+a$, $2p+a$ et $np+a$ pro aequivalentibus haberi possunt; omnia scilicet redeunt ad minimum a, quae reductio cum sit in promtu, eam tuto negligere poterimus, vel tanquam jam factam assumere. Ita si numeri quadrati 1, 4, 9, 16, 25, etc. per numerum p dividantur, nihil obstabit, quominus dicamus residua inde oriunda esse 1, 4, 9, 16, 25, etc. etiamsi hic numeri occurrant ipso divisore p majores. De cetero notandum est, hoc theorema vim suam retinere, sive divisor p sit numerus primus, sive secus.

10. **Coroll. 4.** Cum terminus ultimus pp primi membri nullum praebeat residuum, omnia residua, quae quidem ex tota serie quadratorum oriri possunt, nascentur ex his terminis

$$1,\ 4,\ 9,\ 16,\ \ldots\ (p-1)^2,$$

quorum numerus est $=p-1$.

11. **Coroll. 5.** Plura ergo diversa residua oriri nequeunt, quam $p-1$: quod quidem per se est manifestum. Cum enim omnia residua sint ipso divisore p minora, omnium autem numerorum ipso p minorum numerus sit $=p-1$, etiam numerus residuorum diversorum major esse nequit.

12. **Theorema 3.** Si omnes termini seriei quadratorum 1, 4, 9, 16, etc. per numerum quemcunque p dividantur, ac residua notentur, inter haec residua non omnes numeri minores, quam p, occurrent.

Demonstratio. Omnia enim residua, quae quidem ex divisione omnium quadratorum per numerum p oriuntur, ex his terminis resultant:

$$1,\ 4,\ 9,\ 16\ \ldots\ (p-4)^2,\ (p-3)^2,\ (p-2)^2,\ (p-1)^2,$$

quorum terminorum numerus est $=p-1$: ideoque inde totidem residua proveniunt. Verum haec

residua non omnia inter se sunt diversa: nam terminus ultimus $(p-1)^2 = pp - 2p + 1$ per p divisus residuum relinquit $=1$, idem scilicet, quod primus terminus, 1. Simili modo terminus penultimus $(p-2)^2 = pp - 4p + 4$ idem praebet residuum, quod terminus secundus, 4; et terminus ante penultimus $(p-3)^2$ idem dat residuum, quod terminus tertius, 9. Atque in genere terminus ordine n, qui est nn, idem dat residuum, quod terminus ordine $p-n$, qui est $(p-n)^2$. Cum igitur omnia residua, quae ex his terminis $1, 4, 9 \ldots (p-1)^2$ oriuntur, et quorum numerus est $=p-1$, non sint inter se diversa, in iis non omnes numeri ipso p minores, quorum numerus est $=p-1$, occurrere possunt.

13. **Coroll. 1.** Cum igitur bina residua semper sint aequalia, numerus diversorum residuorum ad semissem $\frac{p-1}{2}$ redigitur, siquidem sit $p-1$ numerus par; at si $p-1$ sit numerus impar, seu p par, tum numerus diversorum residuorum erit $=\frac{p}{2}$: hoc enim casu dabitur residuum medium, quod sui aequale non habet.

14. **Coroll. 2.** Cum igitur omnium numerorum ipso p minorum numerus sit $=p-1$, patet semissem horum numerorum in residuis locum habere; dabunturque ergo numeri, qui ex divisione numerorum quadratorum per numerum p nunquam relinquentur, solo excepto casu, quo $p=2$; quia $p-1=\frac{p}{2}=1$.

15. **Coroll. 3.** Quicunque ergo praeterea sit numerus p, per quem numeri quadrati dividantur, ex numeris ipso p minoribus, semper erunt ad minimum $\frac{p-1}{2}$, vel $\frac{p}{2}$ numeri, qui inter residua non reperiuntur. Prior casus valet, si p est numerus impar, posterior, si par.

16. **Coroll. 4.** Hinc igitur numeri ipso divisore p minores, quorum multitudo est $=p-1$, sponte se in duas classes discriminant, quarum altera continet numeros in residuis locum habentes, altera vero eos, qui in classe residuorum non occurrunt. Hos numeros non-residua hic appellabo.

17. **Scholion.** Quo haec clarius percipiantur, juvabit nonnulla exempla, in quibus residua et non-residua distinguuntur, inspexisse.

Sit	$p=3$	$p=4$	$p=5$	$p=6$	$p=7$
	1, 4	1, 4, 9	1, 4, 9, 16	1, 4, 9, 16, 25	1, 4, 9, 16, 25, 36
residua	1, 1	1, 0, 1	1, 4, 4, 1	1, 4, 3, 4, 1	1, 4, 2, 2, 4, 1
non-resid.	2	2, 3	2, 3	2, 5	3, 5, 6

Sit	$p=8$	$p=9$	$p=10$
	1, 4, 9, 16, 25, 36, 49	1, 4, 9, 16, 25, 36, 49, 64	1, 4, 9, 16, 25, 36, 49, 64, 81
residua	1, 4, 1, 0, 1, 4, 1	1, 4, 0, 7, 7, 0, 4, 1	1, 4, 9, 6, 5, 6, 9, 4, 1
non-resid.	2, 3, 5, 6, 7	2, 3, 5, 6, 8	2, 3, 7, 8

Sit	$p=11$	$p=12$
	1, 4, 9, 16, 25, 36, 49, 64, 81, 100	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121
residua	1, 4, 9, 5, 3, 3, 5, 9, 4, 1	1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1
non-resid.	2, 6, 7, 8, 10	2, 3, 5, 6, 7, 8, 10, 11.

Hinc perspicitur numerum non-residuorum interdum esse vel $\frac{p-1}{2}$, vel $\frac{p-2}{2}$, prout p fuerit numerus vel par, vel impar; interdum esse etiam majorem, nunquam vero esse minorem, omnino uti demonstratio theorematis postulat.

18. **Theorema 4.** Ut omnia residua, quae ex divisione quadratorum per numerum quemcunque p resultare possunt, inveniantur, tantum opus est quadrata ab unitate usque ad terminum $\left(\frac{p-1}{2}\right)^2$, vel $\left(\frac{p}{2}\right)^2$, prout p fuerit vel numerus impar, vel par, per p dividere.

Demonstratio. Ante jam demonstravimus, omnia residua provenire ex divisione horum terminorum:

$$1,\ 4,\ 9,\ 16,\ \ldots\ldots\ (p-1)^2;$$

deinde vero vidimus, seriem residuorum hinc natorum esse reciprocam, seu ordine retrogrado scriptam eandem manere. Quare residua omnia, quatenus inter se sunt diversa, reperientur, si hujus seriei termini tantum ad medietatem usque capiantur, unde si p sit numerus impar, ideoque $p-1$ par, omnes numeri, qui inter residua occurrunt, prodibunt ex his terminis:

$$1,\ 4,\ 9,\ 16\ \ldots\ldots\ \left(\frac{p-1}{2}\right)^2.$$

Sin autem p sit numerus par, quia superior progressio, habet terminum medium, qui retrogrediendo sibi ipse respondet, residua omnia ex his terminis orientur

$$1,\ 4,\ 9,\ 16\ \ldots\ldots\ \left(\frac{p}{2}\right)^2.$$

19. **Coroll. 1.** Si igitur p sit numerus impar, puta $p=2q+1$, omnia residua ex his tantum quadratis $1,\ 4,\ 9,\ 16\ldots\ldots qq$ cognoscentur. At si p sit numerus par, puta $p=2q$, haec quadrata $1,\ 4,\ 9,\ 16\ldots\ldots qq$ omnia producent residua.

20. **Coroll. 2.** Si haec residua omnia inter se fuerint inaequalia, cum eorum numerus sit $=q$, casu priori, quo $p=2q+1$ et $p-1=2q$, numerus non-residuorum erit $=q$. Casu posteriori, quo $p=2q$ et $p-1=2q-1$, omnium non-residuorum numerus erit $=q-1$.

21. **Coroll. 3.** Si a sit numerus quicunque non major, quam $\frac{p-1}{2}$, vel $\frac{p}{2}$, atque residuum constet, quod ex divisione quadrati aa per numerum p resultat, omnia quadrata in hac forma generali $(np\pm a)^2$ contenta idem praebebunt residuum. At numeri omnes omnino in forma $np\pm a$ includuntur, ita ut a non excedat vel $\frac{p-1}{2}$, vel $\frac{p}{2}$.

22. **Scholion.** Quo indolem numerorum, qui sunt residua, facilius explorare liceat, seriem residuorum repraesentemus his litteris $1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta$, etc. pro divisore p, ita ut numerus horum terminorum sit vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, prout p sit vel numerus impar, vel par. Primo igitur patet, in hac serie $1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon$, etc. occurrere ordine omnes numeros quadratos 1, 4, 9, 16 etc. qui quidem sint ipso numero p minores: reliquos autem esse residua, quae in divisione majorum quadratorum per eundem numerum p relinquuntur. Reliquas proprietates residuorum in sequentibus theorematibus indagabimus.

23. **Theorema 5.** Si in serie residuorum $1,\ \alpha,\ \beta,\ \gamma,\ \delta$, etc. occurrat numerus quicunque r, ibidem quoque reperientur omnes potestates ipsius $r^2,\ r^3,\ r^4,\ r^5$, etc., seu residua, quae ex harum potestatum divisione per numerum propositum p, nascuntur.

Demonstratio. Emergat residuum r ex quadrato aa, ita ut sit $aa = mp + r$; et quadratum $a^4 = (mp + r)^2$ per p divisum idem dabit residuum, quod oritur ex rr; atque ex quadrato $a^6 = (mp + r)^3$ idem oritur residuum, quod ex r^3; similique modo residua quadratorum a^8, a^{10}, a^{12}, etc. convenient cum residuis terminorum r^4, r^5, r^6, etc. At residua ex omnibus quadratis quantumvis magnis oriunda jam proveniunt ex quadratis minimis

$$1,\ 4,\ 9,\ 16\ ,\ \ldots\ldots\ \left(\frac{p-1}{2}\right)^2,\ \text{vel}\ \left(\frac{p}{2}\right)^2,$$

ideoque continentur in serie residuorum 1, α, β, γ, δ, etc. Ergo si in hac serie occurrit numerus r, ibidem quoque occurrent termini r^2, r^3, r^4, r^5, etc. seu residua, quae ex eorum divisione per divisorem propositum p relinquuntur.

24. **Coroll. 1.** Quae igitur potestatum r^2, r^3, r^4, r^5, etc. fuerint minores, quam p, eae ipsae in serie residuorum 1, α, β, γ, δ, etc. reperientur. At altiores potestates sua residua, quae divisae per p relinquunt, ibidem introducent.

25. **Coroll. 2.** Si sit $r = 1$, quia omnes ejus potestates sunt $= 1$, ex iis nonnisi unicus terminus 1 in serie residuorum 1, α, β, γ, δ, etc. nascitur. Neque ergo ex hoc casu novus terminus in serie residuorum cognoscitur.

26. **Coroll. 3.** Quia in serie residuorum plures termini non occurrunt, quam vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, plura quoque residua diversa ex potestatibus r^2, r^3, r^4, r^5, etc. etiamsi in infinitum continuentur, prodire non possunt. Unde infinitae harum potestatum per p divisae aequalia praebebunt residua.

27. **Coroll. 4.** Praebeant ergo hae potestates r^m et r^n idem residuum, atque earum differentia $r^m - r^n$ per numerum p erit divisibilis, seu $r^n(r^{m-n} - 1)$. Unde si factor r^n sit ad p primus, quod evenit si residuum r fuerit ad p primum, alter factor $r^{m-n} - 1$ per p erit divisibilis, ideoque potestas r^{m-n} per p divisa unitatem relinquet.

28. **Coroll. 5.** Dabitur ergo potestas r^λ, quae per p divisa unitatem relinquit, quae utique in serie residuorum continetur, siquidem r sit numerus ad p primus. Tum autem potestas $r^{\lambda+1}$ dabit residuum r, potestas $r^{\lambda+2}$ residuum r^2, et $r^{\lambda+3}$ residuum r^3 etc. sicque hae potestates altiores eadem residua reproducunt, quae potestates inferiores r, r^2, r^3, etc.

29. **Coroll. 6.** Cum igitur plura residua diversa provenire nequeant, quam vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, patet, dari numerum λ, non majorem, quam $\frac{p-1}{2}$, vel $\frac{p}{2}$, ita ut potestas r^λ per p divisa unitatem relinquat.

30. **Scholion.** Hinc ergo intelligitur, quomodo fieri possit, ut etiamsi potestates r^2, r^3, r^4, r^5, etc. in infinitum progrediantur, tamen ex iis residua numero finita oriantur, si per divisorem p dividantur. Demonstravi quidem in dissertatione superiori (?), si r sit numerus ad p primus, dari semper ejusmodi potestatem r^λ, quae per p divisa unitatem relinquat, ita ut sit $\lambda < p$. Nunc autem videmus, si r jam in serie residuorum ex quadratis natorum contineatur, tum exponentem λ etiam minorem fieri, quam $\frac{p}{2}$.

31. **Theorema 6.** Si in serie residuorum 1, α, β, γ, δ, etc., quae ex divisione numerorum quadratorum per numerum p oriuntur, occurrant numeri r et s, ibidem quoque occurret horum numerorum productum rs, vel residuum quod ex ejus divisione per numerum p enascitur.

Demonstratio. Proveniet residuum r ex quadrato aa, et residuum s ex quadrato bb, erit $aa = mp + r$, et $bb = np + s$; hinc fiet quadratum $aabb = mnpp + msp + nrp + rs$, quod ergo per p divisum, residuum relinquet rs, vel si $rs > p$, idem relinquet residuum, quod oritur ex rs. Quare cum residuum ex quadrato $aabb$ natum in serie residuorum contineatur, ibi quoque rs, seu residuum inde ortum reperietur.

32. **Coroll. 1.** In serie ergo residuorum 1, α, β, γ, δ, etc. si occurrant duo numeri r et s, ibidem quoque occurrent non solum potestates r, r^2, r^3, r^4, etc. et s, s^2, s^3, s^4, etc. sed etiam producta ex binis terminis quibuscunque rs, r^2s, rs^2, r^3s, r^2s^2, rs^3, etc.

33. **Coroll. 2.** Hinc igitur patet, si formula $\frac{1}{(1-r)(1-s)}$ in seriem resolvatur

$$1 + r + s + rr + rs + ss + r^3 + rrs + rss + s^3 + \text{etc.}$$

singulos terminos hujus seriei in serie residuorum occurrere, vel etiam residua ex his terminis, divisione per p orta.

34. **Coroll. 3.** Etiamsi autem horum terminorum numerus sit infinitus, tamen constat, plura ex iis residua diversa produci non posse, quam vel $\frac{p-1}{2}$, vel $\frac{p}{2}$, prout p fuerit numerus vel impar, vel par.

35. **Schollon.** Quo clarius appareat, quomodo ex his terminis numero infinitis, tamen residuorum diversorum numerus finitus et quidem non major, quam $\frac{p-1}{2}$, vel $\frac{p}{2}$ oriatur, evolvamus exemplum aliquod, sitque $p = 19$, erit $\frac{p-1}{2} = 9$, unde

ex his quadratis	1,	4,	9,	16,	25,	36,	49,	64,	81
orientur residua	1,	4,	9,	16,	6,	17,	11,	7,	5.

Ex hac serie residuorum contemplemur hos duos numeros 5 et 6, ex quibus formemus primo series potestatum

5,	25,	125,	625,	3125,	15625,	78125,	etc.
6,	36,	216,	1296,	7776,	46656,	279936,	etc.

Ex illa serie per $p = 19$ divisa prodeunt residua:

5, 6, 11, 17, 9, 7, 16, 4, 1,

sequens scilicet residuum semper invenitur, si praecedens per 5 multiplicetur, et productum, si sit > 19, infra 19 deprimatur. Simili modo ex potestatibus numeri 6 haec prodibunt residua:

6, 17, 7, 4, 5, 11, 9, 16, 1.

Porro si haec singula residua per singula superiora multiplicentur, et producta infra 19 deprimantur, iidem prodeunt numeri; multiplicetur enim inferior series primo per 5, tum per 6, 11, 17, etc. ut sequitur:

per 5:	11,	9,	16,	1,	6,	17,	7,	4,	5,
per 6:	17,	7,	4,	5,	11,	9,	16,	1,	6,
per 11:	9,	16,	1,	6,	17,	7,	4,	5,	11,
per 17:	7,	4,	5,	11,	9,	16,	1,	6,	17,
per 9:	16,	1,	6,	17,	7,	4,	5,	11,	9,
per 7:	4,	5,	11,	9,	16,	1,	6,	17,	7,
per 16:	1,	6,	17,	7,	4,	5,	11,	9,	16,
per 4:	5,	11,	9,	16,	1,	6,	17,	7,	4,

Perspicitur igitur, quomodocunque hi numeri 1, 4, 9, 16, 6, 17, 11, 7, 5 seriem residuorum constituentes, inter se per multiplicationem combinentur, siquidem divisione per 19 facta infra 19 deprimantur, eosdem semper numeros recurrere, neque unquam ullum numerum eorum, qui non sunt residua, nempe 2, 3, 8, 10, 12, 13, 14, 15, 18 prodire.

36. **Coroll. 4.** Si ergo sit $1, \alpha, \beta, \gamma, \delta$, etc. series residuorum omnium, quae ex divisione quadratorum per numerum p resultant, in eadem serie quoque occurrent omnia producta ex binis pluribusve numerorum $\alpha, \beta, \gamma, \delta$, etc. Ergo si haec expressio $\frac{1}{(1-\alpha)(1-\beta)(1-\gamma)(1-\delta)\,\text{etc.}}$ in seriem evolvatur, omnes ejus termini in serie residuorum occurrent.

37. **Theorema 7.** Si in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc. quae ex divisione quadratorum per numerum p prodeunt, reperiantur numeri r et rs, qui sint ad p primi, quorum ille hujus est factor, tunc in eadem residuorum serie etiam numerus s continebitur.

Demonstratio. Proveniat residuum r ex quadrato aa, et rs ex bb, erit $aa = mp + r$, et $bb = np + rs$: unde fit $bb - aas = np - mps$, sicque $bb - aas$ erit per p divisibile. At cum r et rs sint numeri ad p primi, erunt quoque quadrata aa et bb ad p prima, unde si haec quadrata aa et bb inter se non sint prima, per communem divisorem quadratum ad prima reduci poterunt, ita ut $bb - aas$ maneat per p divisibile. Sint ergo b et a numeri inter se primi, atque cum etiam haec forma $(mp \pm b)^2 - aas$ sit per p divisibilis, semper pro m ejusmodi numerus assignari potest, ut fiat $mp \pm b$ multiplum ipsius a. Sit ergo $mp \pm b = ac$, erit $aacc - aas$ per p divisibile, quod cum sit $= aa(cc - s)$, alterque factor aa sit ad p primus, necesse est, ut alter factor $cc - s$ per p sit divisibilis, unde quadratum cc per p divisum relinquet s, ex quo numerus s in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc. reperietur, siquidem ibi numeri r et rs occurrant, iique sint ad p primi.

38. **Coroll. 1.** Ut igitur veritas theorematis consistat, necesse est, ut numeri r et rs, seu r et s sind ad divisorem p primi. Supra enim vidimus, si sit $p = 12$, in residuis reperiri numeros 4 et 0, seu 4 et 12, hinc autem, posito $r = 4$ et $rs = 12$, non sequitur numerum $s = 3$ in residuis reperiri: quia r et s non sunt numeri ad p primi: ac revera etiam numerus 3 inter non-residua continetur.

39. **Coroll. 2.** Sin autem divisor p sit numerus primus, quia tum omnia residua $\alpha, \beta, \gamma, \delta$, etc. ad eum sunt prima, si in iis occurrant numeri r et rs, tum etiam certo in iis occurret numerus s.

40. **Coroll. 3.** Si inter residua occurrant numeri r et s primi ad p, quia residuo r aequivalentia censenda sunt residua $p + r$, $2p + r$, et in genere $np + r$, si fuerit $np + r = ts$, tum etiam numerus t inter residua reperietur.

41. **Scholion.** Ne ad hujusmodi exceptiones, quando residua non sunt numeri ad p primi, respicere obligemur, in sequentibus ponamus divisorem p semper esse numerum primum; et cum residua ex binario orta sint obvia, sit divisor p simul numerus impar, seu $p = 2q + 1$, tum ergo series residuorum formabitur ex his terminis:

$$1,\ 4,\ 9,\ 16,\ \ldots\ \ldots\ qq$$

ita ut eorum numerus, quatenus inter se sunt diversa, major esse nequeat, quam q. Si igitur residua ex hoc divisore primo $p = 2q + 1$ sint 1, α, β, γ, δ, etc. in hac serie non solum producta ex binis pluribusve terminorum α, β, γ, δ, etc. occurrent, sed quia omnia haec residua ad p sunt prima, si inter ea occurrant r et rs, ita ut unum per aliud sit divisibile, tum etiam quotus inde natus s in eadem serie residuorum continebitur.

42. **Theorema 8.** Si ex divisore primo $p = 2q + 1$, per quem omnes numeri quadrati dividantur, nascatur series residuorum 1, α, β, γ, δ, ε, etc., quorum numerus est $= q$, omnia haec residua inter se erunt inaequalia.

Demonstratio. Primo patet, nullum residuum in hac serie esse posse $= 0$, cum enim nascantur ex quadratis ipso qq non majoribus, nullum horum quadratorum per numerum primum $p = 2q + 1$ est divisibile; igitur cyphra inter residua multo minus bis occurrere poterit. Ponamus autem duo residua, quae ex quadratis aa et bb oriuntur, esse aequalia, eritque differentia horum quadratorum $aa - bb$ per divisorem $p = 2q + 1$ divisibilis. At cum omnia haec residua 1, α, β, γ, δ, etc. ex quadratis minimis, quae qq non excedunt, oriantur, quadrata illa aa et bb non superabunt qq, eritque propterea neque $a > q$, neque $b > q$, neque idcirco $a + b > 2q$; unde certo erit $a + b < p$. Cum igitur differentia quadratorum $aa - bb$ esset per p divisibilis, siquidem residua inde nata essent aequalia, et p sit numerus primus, vel summa $a + b$, vel differentia $a - b$ foret per p divisibilis; utrumque autem, ob tam $a - b < p$, quam $a + b < p$, fieri nequit. Ergo omnia residua, quae ex divisione quadratorum 1, 4, 9, $16, \ldots qq$ per numerum primum $p = 2q + 1$ resultant, inter se sunt inaequalia.

43. **Coroll. 1.** Numerus igitur omnium residuorum diversorum, quae ex divisione quadratorum per numerum primum $p = 2q + 1$ oriuntur, certo est $= q$; ante enim ostensum est, eum non esse majorem, quam q; hic autem evicimus, eum non esse minorem, quam q.

44. **Coroll. 2.** Cum numerus omnium numerorum ipso divisore $p = 2q + 1$ minorum sit $= p - 1 = 2q$, patet, horum numerorum semissem tantum in serie residuorum 1, α, β, γ, etc. occurrere eamque constituere, alterum vero semissem, constituere seriem non-residuorum: ideoque si p sit numerus primus, seriem non-residuorum etiam ex q numeris constare.

45. **Coroll. 3.** Si ergo x sit numerus quicunque ex serie non-residuorum divisori p respondentium, certo affirmare possumus, quicquid sit n, nullum numerum in hac forma $np + x$ esse posse quadratum.

46. **Scholion.** Quia nunc investigationes nostras tantum ad divisores primos dirigimus, expediet tam residua, quam non-residua, quae minoribus numeris primis respondent hic exhibere. In genere scilicet si divisor sit p, seriem residuorum per $1,\ \alpha,\ \beta,\ \gamma,\ \delta$, etc. et seriem non-residuorum per $a,\ b,\ c,\ d,\ e$, etc. repraesentamus; et quo facilius conjunctim tam residua, quam non-residua, referantur, hoc modo exponemus:

$$p\left\{\begin{matrix}1, & \alpha, & \beta, & \gamma, & \delta, & \epsilon, & \zeta, & \text{etc.}\\ a, & b, & c, & d, & e, & f, & g, & \text{etc.}\end{matrix}\right\}.$$

duas nimirum series numerorum quovis casu scribemus, quarum superior residua, inferior non-residua continet, et utrique divisorem p, ad quem pertinent, praefigemus. Hoc modo residua et non-residua, quae ex divisoribus primis simplicioribus resultant, ita indicabuntur:

$$3\left\{\begin{matrix}1\\2\end{matrix}\right\},\quad 5\left\{\begin{matrix}1, & 4\\2, & 3\end{matrix}\right\},\quad 7\left\{\begin{matrix}1, & 4, & 2\\3, & 5, & 6\end{matrix}\right\},\quad 11\left\{\begin{matrix}1, & 4, & 9, & 5, & 3\\2, & 6, & 7, & 8, & 10\end{matrix}\right\},\quad 13\left\{\begin{matrix}1, & 4, & 9, & 3, & 12, & 10\\2, & 5, & 6, & 7, & 8, & 11\end{matrix}\right\},$$

$$17\left\{\begin{matrix}1, & 4, & 9, & 16, & 8, & 2, & 15, & 13\\3, & 5, & 6, & 7, & 10, & 11, & 12, & 14\end{matrix}\right\},\qquad 19\left\{\begin{matrix}1, & 4, & 9, & 16, & 6, & 17, & 11, & 7, & 5\\2, & 3, & 8, & 10, & 12, & 13, & 14, & 15, & 18\end{matrix}\right\},$$

$$23\left\{\begin{matrix}1, & 4, & 9, & 16, & 2, & 13, & 3, & 18, & 12, & 8, & 6\\5, & 7, & 10, & 11, & 14, & 15, & 17, & 19, & 20, & 21, & 22\end{matrix}\right\},\quad 29\left\{\begin{matrix}1, & 4, & 9, & 16, & 25, & 7, & 20, & 6, & 23, & 13, & 5, & 28, & 24, & 22\\2, & 3, & 8, & 10, & 11, & 12, & 14, & 15, & 17, & 18, & 19, & 21, & 26, & 27\end{matrix}\right\}.$$

Residua hic eo ordine, quo ex quadratis nascuntur, sunt posita, non-residua autem, quia nullo ordine connectuntur, a minimis ad majora progrediendo collocavimus. Exempla haec quoque in eum finem servire poterunt, ut in iis proprietates residuorum ante demonstratae examinentur.

47. **Theorema 9.** Si ex divisione quadratorum per numerum primum $p=2q+1$ nascatur haec series residuorum, $1,\ \alpha,\ \beta,\ \gamma,\ \delta$, etc. haecque series non-residuorum $a,\ b,\ c,\ d,\ e$, etc. atque in hac serie non-residuorum occurrat numerus r, in eadem quoque occurrent omnes hi numeri $\alpha r,\ \beta r,\ \gamma r,\ \delta r$, etc. vel eorum residua divisione per p relicta.

Demonstratio. Quicunque enim horum numerorum, ut αr, vel in serie residuorum continetur, vel in serie non-residuorum. At cum α in serie residuorum contineatur, si αr ibidem contineretur, necessario quoque r in serie residuorum existeret. Quare cum per hypothesin r sit numerus ex serie non-residuorum, numerus αr non erit in serie residuorum, habebit ergo αr locum in serie non-residuorum, quod idem de numeris $\beta r,\ \gamma r,\ \delta r$, etc. valet: Quod autem demonstravimus de his productis $\beta r,\ \gamma r,\ \delta r$, etc. si sint majora, quam p, id intelligendum est de residuis, quae haec producta per p divisa relinquunt.

48. **Coroll. 1.** Quia omnes numeri $1,\ \alpha,\ \beta,\ \gamma,\ \delta$, etc., quorum numerus est $=q$, sunt inter se diversi, sequitur quoque, omnes hos numeros $r,\ \alpha r,\ \beta r,\ \gamma r,\ \delta r$, etc. esse inter se diversos: unde, si omnia residua habeantur, ex unico non-residuo cognito reliqua omnia non-residua definiuntur.

49. **Coroll. 2.** Dabit ergo series r, αr, βr, γr, δr, etc. omnia plane non-residua; continet enim q numeros diversos, totidemque et non plura existunt non-residua, siquidem divisor p est numerus primus.

50. **Coroll. 3.** Si ergo ex serie non-residuorum quilibet alius numerus s capiatur, ejus producta αs, βs, γs, etc. alios numeros pro residuis non praebent, nisi qui ex quovis alio r hoc modo sunt reperti.

51. **Theorema 10.** Producta ex binis numeris seriei non-residuorum continentur in serie residuorum, siquidem haec residua nascantur ex divisione numerorum quadratorum per quempiam numerum primum.

Demonstratio. Sit enim $p = 2q + 1$ divisor primus, atque series residuorum sit 1, α, β, γ, δ, etc., series autem non-residuorum sit a, b, c, d, e, etc. Vidimus autem, si r sit non-residuum quodcunque, seriem non-residuorum hoc modo quoque exhiberi: r, αr, βr, γr, δr, etc. Jam productum ex duobus quibuscunque horum terminorum $\alpha\beta r^2$, constat ex duobus factoribus $\alpha\beta$ et rr, quorum uterque in serie residuorum continetur, quia omnia quadrata, ac propterea etiam rr ibi occurrunt; unde perspicuum est, productum ex binis quibusque non-residuis in serie residuorum contineri.

52. **Coroll. 1.** Ut igitur productum ex duobus residuis dat residuum, ita quoque productum ex duobus non-residuis dabit residuum. Sed productum ex residuo et non-residuo semper producit non-residuum.

53. **Coroll. 2.** Hinc etiam sequitur, uti residuum per residuum divisum dat residuum, ita quoque non-residuum per non-residuum divisum dare residuum. Verum residuum per non-residuum, vel vicissim non-residuum per residuum divisum praebet non-residuum.

54. **Coroll. 3.** Quemadmodum bina non-residua invicem multiplicata residuum producunt, ita terna non-residua invicem multiplicata praebebunt non-residuum: quaterna vero non-residua iterum residuum producunt, at quina non-residuum, et sic deinceps.

55. **Definitio.** Complementum residui est ejus defectus a divisore, ex quo est ortum: sic si divisor sit $= p$ et residuum $= r$, erit complementum residui $= p - r$.

56. **Coroll. 1.** Quia ratione residuorum omnes hi numeri r, $p + r$, $2p + r$, et in genere $np + r$ pro iisdem habentur, quicunque numerus pro n sumatur, erit eorum complementum $= p - np - r$, unde si sumatur $n = 1$, complementum residui r erit $= -r$.

57. **Coroll. 2.** Si n sumatur $= -1$, residuum r etiam per $r - p$ exprimi potest, ita ut sit negativum. In divisione enim, si quotus nimis magnus accipitur, ad residua negativa pervenitur. Sic residuum affirmativum r aequivalebit residuo negativo $r - p$.

58. **Coroll. 3.** Si sit $r > \frac{1}{2}p$, tum hoc residuum negative exprimi poterit per $r - p$, quod erit minus, quam $\frac{1}{2}p$. Ita si expressiones negativae in usum vocentur, omnia residua per numeros exhiberi poterunt, semisse divisoris $\frac{1}{2}p$ non majores. Sic pro divisore $p = 23$ habebuntur haec residua per numeros non majores, quam $\frac{23}{2}$ expressa: $1, 4, 9, -7, 2, -10, 3, -5, -11, 8, 6$.

59. **Coroll. 4.** Similique modo non-residua etiam per numeros ipso $\frac{1}{2}p$ non majores exhiberi poterunt, eruntque pro divisore $p = 23$ haec non-residua: 5, 7, 10, 11, -9, -8, -6, -4, -3, -2, -1. Unde si $p = 2q + 1$, numerus tam residuorum, quam non-residuorum, erit $= q$, neque in utraque serie occurrunt numeri majores, quam q.

60. **Coroll. 5.** Si hoc modo residua exprimantur, statim patet, utrum cujuspiam residui complementum in eadem serie residuorum contineatur, nec ne. Nempe si r sit residuum, erit $-r$ ejus complementum, et vicissim si $-r$ sit residuum, erit $+r$ ejus complementum. Quare nisi in serie residuorum idem numerus bis occurrat, affirmative scilicet et negative, ejus complementum in serie residuorum non continetur.

61. **Theorema 11.** Si in serie residuorum 1, α, β, γ, δ, etc., quae ex divisione quadratorum per numerum primum $p = 2q + 1$ generantur, unius termini occurrat complementum, tum simul omnium terminorum complementa in eadem serie occurrent.

Demonstratio. Sit r id residuum, cujus complementum $-r$ quoque in serie 1, α, β, γ, δ, etc. occurrat. Cum igitur $-r$ per r divisum det -1, in eadem serie quoque numerus -1 occurret: seu valor cujuspiam litterarum α, β, γ, δ, etc. erit $= -1$. Quoniam ergo in eadem serie producta ex binis terminis simul reperiuntur, ibidem occurrent termini $-\alpha$, $-\beta$, $-\gamma$, $-\delta$, etc. Cujusvis ergo residui complementum simul in serie residuorum reperietur, siquidem unici termini complementum in ea occurrat.

62. **Coroll. 1.** Si ergo unici termini r complementum $-r$ in serie residuorum contineatur, tum quilibet numerus hujus seriei bis occurret, primo scilicet affirmative, tum vero etiam negative. In serie nempe residuorum 1, α, β, γ, δ, etc. etiam continebuntur termini -1, $-\alpha$, $-\beta$, $-\gamma$, $-\delta$, etc.

63. **Coroll. 2.** Cum igitur hoc casu in serie residuorum quilibet terminus bis occurrat, numerus omnium terminorum necessario erit par. At numerus omnium terminorum est $= q$, ergo nisi sit q numerus par, fieri nequit, ut complementa residuorum simul in serie residuorum contineantur.

64. **Coroll. 3.** Si igitur q est numerus impar, puta $q = 2n + 1$, ita ut sit $p = 4n + 3$, in serie residuorum nullus plane occurrit numerus, cujus complementum simul in ea serie contineatur. Omnia ergo complementa hoc casu in seriem non-residuorum ingredientur, eritque utrinque terminorum numerus impar $= q = 2n + 1$.

65. **Scholion.** Hinc ergo summum discrimen agnoscitur, quod inter numeros primos $p = 2q + 1$ intercedit, prout q fuerit numerus par, vel impar: cum posteriori casu certo sciamus, nullius residui complementum in residuorum serie contineri. Quodsi ergo priori casu ponamus $q = 2n$, posteriori $q = 2n - 1$, illo casu erit numerus primus $p = 4n + 1$, hoc vero $p = 4n - 1$; unde patet, omnes numeros primos, binario excepto, vel unitate superare multiplum quaternarii, vel unitate ab eo deficere; sicque duas obtinemus numerorum classes, quarum altera in forma $4n + 1$, altera in forma $4n - 1$, continetur. Prioris classis $4n + 1$ sunt ergo numeri primi: 5, 13, 17, 29, 37, 41,

53, 61, 73, 89, 97, etc., posterioris vero classis $4n-1$ hi: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83. De numeris primis classis prioris Fermatius olim pronunciavit, singulos esse aggregata duorum quadratorum, cujus theorematis veritatem nuper tandem post plures conatus demonstravi. De numeris autem posterioris classis facile ostenditur, nullum eorum esse summam duorum quadratorum; quin etiam mox demonstrabo, ne quidem summam duorum quadratorum $aa+bb$ exhiberi posse, quae sit per ejusmodi numerum primum $p=4n-1$ divisibilis, nisi utrumque quadratum aa et bb seorsim per eum divisibile existat. De his tamen numeris Fermatius affirmavit, singulos vel esse trium, vel quatuor quadratorum aggregata; ita videmus esse $3=1+1+1$, $7=1+1+1+4$, $11=1+1+9$, $19=1+9+9$, $23=1+4+9+9$, $31=4+9+9+9=1+1+4+25$, etc. Verum nullum existere hujusmodi numerum, qui non ad minimum in quatuor quadrata resolvi possit, etsi Fermatius ejus demonstrationem se invenisse sit professus, tamen nusquam eam publicavit, ita ut cum ipso penitus interiisse videatur, neque deinceps quisquam inventus est, qui hanc demonstrationem, quae in analysi Diophantea et universa numerorum scientia maximi est momenti, reperire potuerit. Equidem hic demonstrabo, quocunque proposito numero primo formae $4n-1$, semper summam quatuor quadratorum, quin etiam trium, exhiberi posse, quae per eum sit divisibilis. Cum igitur etiam demonstrari queat, producta ex duobus numeris, quorum uterque est summa quatuor quadratorum, etiam esse quatuor quadratorum aggregata, non procul a demonstratione desiderata abesse videmur. Tantum enim superest, ut demonstretur, si summa quatuor quadratorum fuerit divisibilis per numerum, qui etiam sit summa quatuor quadratorum, quotum quoque certo fore summam quatuor quadratorum.

66. **Theorema 12.** Si omnia quadrata per numerum primum $=4n-1$ dividantur, indeque oriatur series residuorum $1, \alpha, \beta, \gamma, \delta$, etc. nullius residui complementum simul in hac serie residuorum continebitur.

Demonstratio. Omnia residua

$$1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \ldots\ldots\ \nu$$

resultant ex divisione horum quadratorum:

$$1,\ 4,\ 9,\ 16,\ 25,\ \ldots\ldots\ (2n-1)^2$$

per numerum primum $4n-1$. Numerus ergo horum residuorum est $=2n-1$, ideoque impar. At si unius residui α complementum $p-\alpha$ seu $-\alpha$ in eadem serie extaret, tum simul omnium residuorum complementa ibidem occurrere deberent, sicque cum unumcunque residuum bis, nempe cum signo $+$ et cum signo $-$ adesset, numerus residuorum esset par. Quare cum sit impar, fieri nequit, ut vel unici residui complementum simul in eadem residuorum serie contineatur.

67. **Coroll. 1.** Si ultimus seriei residuorum terminus ponatur $=\nu$, quia oritur ex quadrato $(2n-1)^2=4nn-4n+1$ per $4n-1$ diviso, erit residuum $\nu=-3n+1=n$, sumto quoto $n-1$. Ergo ejus complementum $-n$ seu $3n-1$ in serie residuorum non reperitur. Numerus ergo $-n$ seu $3n-1$ certo erit in serie non-residuorum.

68. **Coroll. 2.** Cum $mp-n$ seu $m(4n-1)-n$ omnes numeros complectatur, qui per $4n-1$ divisi residuum dant $-n$, patet nullum horum numerorum $m(4n-1)-n$ seu $4mn-m-n$ unquam esse posse quadratum.

69. **Coroll. 3.** Cum in serie residuorum occurrant numeri quadrati $1, 4, 9, 16$, etc. in eadem certe non occurrent eorum complementa $-1, -4, -9, -16$, etc. Numeri ergo quadrati signo $-$ affecti in seriem non-residuorum ingredientur.

70. **Theorema 13.** Non datur summa duorum quadratorum, quae sit divisibilis per numerum primum formae $4n-1$, nisi utrumque quadratum seorsim per eundem sit divisibile: seu non datur summa duorum quadratorum inter se primorum per numerum primum $4n-1$ divisibilis.

Demonstratio. Ponamus enim summam duorum quadratorum $aa+bb$ esse per numerum primum $4n-1$ divisibilem, neque tamen vel aa vel bb seorsim esse per $4n-1$ divisibile. Sit ergo r residuum, quod in divisione quadrati aa per $4n-1$ relinquitur, et s residuum ex divisione quadrati bb ortum; atque tam r quam s in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc. occurret. Jam summa quadratorum $aa+bb$ per $4n-1$ divisa relinquit residuum $r+s$, quod cum per hypothesin esse debeat $=$ divisori $4n-1$, erit $s=4n-1-r$, seu $s=-r$, ideoque s erit complementum residui r. Quare si r in serie residuorum contineatur, ejus complementum s in ea certe non occurret: unde sumto quadrato quocunque aa, nullum datur aliud quadratum bb ejusmodi, ut summa $aa+bb$ fiat per numerum primum $4n-1$ divisibilis, nisi ipsum quadratum aa per se sit divisibile per $4n-1$; quo casu etiam bb per $4n-1$ divisibile esse debet. Nulla ergo datur summa duorum quadratorum inter se primorum, quae sit per numerum primum $4n-1$ divisibilis.

71. **Coroll. 1.** Non ergo datur hujusmodi formae $aa+1$ numerus, qui sit per numerum primum $4n-1$ divisibilis. Ad hoc enim opus esset, ut residuum ex quadrato bb ortum esset $=-1$, quod autem in serie residuorum non existit.

72. **Coroll. 2.** Cum summa duorum quadratorum $aa+bb$ per nullum numerum primum formae $4n-1$ sit divisibilis, etiam per nullum numerum compositum p, qui factorem primum habet formae $4n-1$, erit divisibilis; si enim per hunc numerum p esset divisibilis, etiam per ejus factorem $4n-1$ divisibilis foret.

73. **Theorema 14.** Sive numerus $4n-1$ sit primus, sive compositus, nulla datur summa duorum quadratorum, inter se primorum, per eum numerum $4n-1$ divisibilis.

Demonstratio. Si enim numerus $4n-1$ sit primus, jam demonstrata est veritas theorematis. At si $4n-1$ non sit numerus primus, erit productum ex aliquot numeris primis, et quidem imparibus, cum ipse numerus $4n-1$ sit impar. Omnes autem numeri primi sunt vel formae $4m+1$, vel $4m-1$: sed omnes factores numeri $4n-1$ esse nequeunt formae $4m+1$; quotcunque enim numeri hujus formae $4m+1$ in se invicem multiplicentur, productum semper erit numerus formae $4n+1$, seu unitate excedet multiplum quaternarii. Quare necesse est, ut numerus $4n-1$ unum ad minimum habeat factorem primum formae $4m-1$, et quia per talem numerum primum nulla summa duorum quadratorum inter se primorum est divisibilis, nulla etiam datur, quae per numerum compositum $4n-1$ esset divisibilis.

74. **Coroll. 1.** Cum nulla detur summa duorum quadratorum inter se primorum per numerum $4n-1$, sive sit primus, sive compositus, divisibilis, multo minus numerus $4n-1$ ipse erit summa duorum quadratorum. Si enim esset $4n-1=aa+bb$, utrumque quadratum aa et bb seorsim per $4n-1$ divisibile esse deberet, quod, cum utrumque sit minus quam $4n-1$, fieri nequit.

75. **Scholion.** Nullum numerum formae $4n-1$ esse posse summam duorum quadratorum, etiam facillime hoc modo ostenditur. Si enim numerus $4n-1$ esset summa duorum quadratorum, alterum esse deberet par, alterum impar. At omnia quadrata paria sunt numeri hujus formae $4f$, et omnia quadrata imparia numeri hujus formae $4g+1$. Summa ergo duorum quadratorum, quorum alterum est par, alterum impar, erit numerus formae $4f+4g+1$, seu $4n+1$; ergo numerus formae $4n-1$ non potest esse summa duorum quadratorum.

76. **Coroll. 2.** Nullus etiam numerus, qui factorem habet formae $4n-1$, potest esse divisor summae duorum quadratorum inter se primorum: si enim esset divisor, etiam ejus factor $4n-1$, foret divisor, quod fieri nequit.

77. **Coroll. 3.** Multo ergo minus hujusmodi numerus, qui factorem habet $4n-1$, esse potest summa duorum quadratorum inter se primorum. Ita impossibile est, ut sit $m(4n-1)=aa+bb$, si quidem a et b sint numeri inter se primi.

78. **Theorema 15.** Nullus numerus in hac forma $4mn-m-n$ contentus, quicunque numeri pro m et n capiantur, unquam esse potest quadratum.

Demonstratio. Cum nullus numerus, qui factorem habet $4n-1$, esse queat summa duorum quadratorum inter se primorum, seu quae praeter unitatem nullum habeant communem divisorem, sequitur fieri non posse, ut sit $(4m-1)(4n-1)=1+aa$. Ergo non erit $16mn-4m-4n=aa$: unde ne ejus quadrans quidem $4mn-m-n$ unquam quadratum esse potest.

79. **Theorema 16.** Si in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc., quae ex divisione quadratorum per numerum quemcunque p resultant, cujuspiam residui complementum in eadem serie residuorum occurrat, tum duo quadrata exhiberi poterunt, quorum summa sit per eundem numerum p divisibilis, etiamsi neutrum seorsim per p sit divisibile.

Demonstratio. Praebeat quadratum aa residuum $=r$, quadratum autem bb residuum $=-r$, seu $p-r$, quod illius est complementum, ita ut r sit id residuum, cujus complementum simul in serie residuorum contineatur. Jam manifestum est, summam horum quadratorum $aa+bb$ fore per numerum p divisibilem.

80. **Coroll. 1.** Si p sit numerus primus, statim atque unius residui complementum in serie residuorum occurrit, etiam singulorum residuorum complementa ibidem inerunt. Sumto ergo quadrato quocunque aa, cujus residuum sit $=r$, dabitur aliud xx, cujus residuum erit $=-r$, ita ut x sit non majus, quam $\frac{p}{2}$, atque summa $aa+xx$ erit per p divisibilis.

81. **Coroll. 2.** Si igitur detur summa duorum quadratorum $aa+bb$ per numerum primum p divisibilis, quia residuorum ex aa et bb ortorum alterum alterius est complementum; residui ex

quocunque alio quadrato cc orti complementum in serie residuorum quoque reperietur. Dabitur ergo summa duorum quadratorum $cc + xx$ per numerum p divisibilis.

82. **Coroll. 3.** Ex praecedentibus autem patet, hunc casum locum obtinere non posse, neque si p sit numerus formae $4n - 1$, neque si p saltem habeat factorem hujus formae: quia neutro casu datur summa duorum quadratorum per p divisibilis, quae quidem quadrata sint inter se prima.

83. **Coroll. 4.** Nulli ergo alii numeri primi relinquuntur, ad quos theorema hoc accommodari queat, nisi qui contineantur in hac forma $4n + 1$.

84. **Scholion.** An autem omnes numeri primi formae $4n + 1$ hanc habeant proprietatem, ut in seriebus residuorum inde ortis cujusque termini complementum simul ibidem reperiatur, hic nondum est demonstratum, neque desperandum videtur, quin ex his iisdem principiis demonstratio elici queat, etsi nondum mihi quidem eo pertingere licuit. Series autem residuorum, ex simplicioribus numeris primis hujus formae ortae, sequenti modo se habent, ubi quidem residua, semisse cujusque numeri majora, per numeros negativos exhibere visum est, quo facilius, quaenam sint aliorum complementa, appareat:

$$5\{1, -1\}; \quad 13\{1, 4, -4, 3, -1, -3\}; \quad 17\{1, 4, -8, -1, 8, 2, -2, -4\};$$

$$29\{1, 4, 9, -13, -4, 7, -9, 6, -6, 13, 5, -1, -5, -7\};$$

$$37\{1, 4, 9, 16, -12, -1, 12, -10, 7, -11, 10, -4, -16, 11, 3, -3, -7, -9\}.$$

In his igitur seriebus perspicuum est cujusque termini complementum simul in iis occurrere. Quod autem hoc necessario eveniat, si divisor sit numerus primus formae $4n + 1$, demonstratio directa adhuc desideratur, quae hoc modo institui debere videtur. Prodeat ex numero primo $4n + 1$ haec series residuorum $1, \alpha, \beta, \gamma, \delta$, etc., quorum terminorum numerus est $2n$, jam si quis neget horum terminorum complementa simul in eadem serie contineri, is dicere debet, omnia complementa $-1, -\alpha, -\beta, -\gamma, -\delta$, etc. seriem non-residuorum constituere; quorum terminorum numerus cum sit $= 2n$, sequeretur, nulla alia praeterea dari non-residua, quare, si assignari posset quispiam numerus, in serie non-residuorum contentus, qui non esset complementum cujuspiam termini in serie residuorum contenti, simul sequeretur nullum plane complementum seriei residuorum in serie non-residuorum occurrere. Hoc ergo si demonstrari posset, haberetur demonstratio desiderata, et quidem directa. Nam demonstratio indirecta jam inde datur, quod demonstravi, omnem numerum primum formae $4n + 1$ esse summam duorum quadratorum: quare si sit $4n + 1 = aa + bb$, residuorum ex his quadratis aa et bb ortorum alterum alterius erit complementum, hincque porro recte concluditur, cujusque residui complementum simul in serie residuorum contineri.

85. **Theorema 17.** Si in serie residuorum $1, \alpha, \beta, \gamma, \delta$, etc., quae ex divisione quadratorum per numerum quemcunque p oriuntur, occurrat terminus, qui sit complementum summae duorum aliorum terminorum, tum summa trium quadratorum exhiberi potest per numerum p divisibilis, ita ut nullius quadrati radix major sit quam $\frac{p}{2}$.

Demonstratio. Sint r et s residua ex duobus quadratis aa et bb oriunda, quorum summa $= r + s$, ejusque ergo complementum $= p - r - s$. Jam si hoc complementum in serie residuorum 1, α, β, γ, δ, etc. reperiatur, dabitur quadratum $cc < \frac{1}{4}pp$, quod per p divisum relinquet $-r-s$; sicque manifestum erit, summam horum trium quadratorum $aa + bb + cc$ fore per numerum p divisibilem; neque horum quadratorum ullum majus esse, quam $\frac{1}{4}pp$.

86. **Coroll. 1.** Si igitur in serie residuorum 1, α, β, γ, δ, etc. occurrat aliquis ex his numeris: -2, $-1-\alpha$, -2α, $-1-\beta$, $-\alpha-\beta$, -2β, $-1-\gamma$, $-\alpha-\gamma$, $-\beta-\gamma$, -2γ, $-1-\delta$, $-\alpha-\delta$, etc. semper summa trium quadratorum exhiberi potest per numerum p divisibilis.

87. **Coroll. 2.** Atque si p sit numerus primus, singulorum horum quadratorum radices a, b, c, cum sint minores, quam $\frac{p}{2}$, erunt numeri ad p primi, ideoque etiam ipsa quadrata, ac nisi ipsa haec tria quadrata fuerint prima inter se, sed communem habeant divisorem quadratum, quia hic necesserio est ad p primus, per eum quadrata illa reducentur ad minora et prima inter se, quorum summa pariter per p erit divisibilis.

88. **Coroll. 3.** Si in serie residuorum singulorum terminorum complementa simul insint, tum etiam summa duorum quadratorum assignari potest per numerum p divisibilis. Quando autem duorum quadratorum summa datur, multo magis dabitur summa trium quadratorum, cum forma $aa + bb$ contineatur in forma $aa + bb + cc$.

89. **Scholion.** Simili modo demonstratur, si in serie residuorum occurrat numerus, qui sit complementum summae trium residuorum, tum summam quatuor quadratorum exhiberi posse, quae sit per numerum p divisibilis. Verum si summae binorum vel ternorum residuorum capiantur, tot prodeunt numeri diversi, ut satis manifestum videatur, eorum omnium complementa in serie nonresiduorum contineri non posse.

90. **Theorema 18.** **Proposito quocunque numero primo p, si non duorum quadratorum inter se primorum summa per eum divisibilis exhiberi potest, certo semper summa trium quadratorum per eum divisibilis assignari potest, ita ut non singula seorsim per p sint divisibilia.**

Demonstratio. Sit 1, α, β, γ, δ, ε, etc. series residuorum ex divisione quadratorum per numerum propositum primum p orta. Jam in hac serie vel occurrit -1, vel non occurrit. Si -1 ibi occurrit, singulorum residuorum complementa simul ibi occurrunt, ideoque pluribus modis summa duorum quadratorum per p divisibilis datur. Sin autem -1 non in serie residuorum contineatur, in serie non-residuorum reperietur, ubi simul complementa omnium residuorum occurrent: hoc ergo casu nulla dabitur summa duorum quadratorum per numerum p divisibilis; nisi utrumque seorsim divisorem admittat. Dari autem his casibus summam trium quadratorum per numerum primum p divisibilem, ita ostendo. Primo notetur, si quis numerus r in serie residuorum occurrat, ejus complementum $-r$ certo in serie non-residuorum esse, et vicissim, si r sit non-residuum, certo fore $-r$ residuum. Ponamus jam negari, ullam dari summam trium quadratorum per p divisibilem; et quia in serie residuorum primo adest numerus 1, numerus -2 ibidem non occurret, (alias enim daretur summa trium quadratorum per p divisibilis, contra hyp.) Occurret igitur -2

in serie non-residuorum, ac propterea numerus $+2$ in serie residuorum. Jam cum in serie residuorum habeantur numeri 1 et 2, summae eorum complementum -3, erit non-residuum, ideoque $+3$ residuum. Eodem modo ex residuis 1 et 3 concluditur fore -4 non-residuum, ac proinde $+4$ residuum. Atque in genere si residuum quodcunque sit r, debebit $-r-1$ esse non-residuum, hincque $1+r$ foret residuum. Ex hac ergo hypothesi sequitur, omnes plane numeros 1, 2, 3, 4, 5, 6, etc. in serie residuorum contineri, sicque nullos plane numeros pro serie non-residuorum relinqui, quod cum sit absurdum, concludere debemus dari utique trium quadratorum summam per numerum primum p divisibilem, quorum quidem nullum seorsim sit per p divisibile. Quae si forte non fuerint prima inter se, per eorum maximum communem divisorem ad prima deprimi poterunt, quia maximus communis divisor quadratorum certo est quadratus.

91. **Coroll. 1.** Simili ratiocinio evincitur, multo magis repugnare, si quis negaret, dari quatuor quadratorum summam per numerum primum divisibilem. Ergo proposito numero quocunque primo p, semper dabitur summa quatuor quadratorum per eum divisibilis.

92. **Coroll. 2.** Si numerus primus p non sit divisor ullius summae duorum quadratorum, tria illa quadrata aa, bb, cc, quorum summa $aa+bb+cc$ est per p divisibilis, singula erunt minora, quam $\frac{1}{4}pp$. Hinc ergo erit $aa+bb+cc<\frac{3}{4}pp$, unde quotus, qui ex divisione hujus aggregati $aa+bb+cc$ per p oritur, erit $<\frac{3}{4}p$.

93. **Theorema 19.** Si summa quatuor quadratorum per summam quatuor quadratorum dividatur, quotus erit quoque summa quatuor quadratorum, saltem in fractis.

Demonstratio. Sit $aa+bb+cc+dd$ summa quatuor quadratorum, quae dividenda sit per hanc summam quatuor quadratorum $pp+qq+rr+ss$, erit quotus $=\frac{aa+bb+cc+dd}{pp+qq+rr+ss}$, qui sive sit numerus integer, sive fractus, semper in quatuor quadrata saltem in fractis resolvi potest. Multiplicemus enim numeratorem et denominatorem per $pp+qq+rr+ss$, ut denominator fiat quadratus, erit quotus iste $=\frac{(aa+bb+cc+dd)(pp+qq+rr+ss)}{(pp+qq+rr+ss)^2}$; quod si jam numerator in quatuor quadrata resolvi queat, ipsa fractio aequabitur aggregato quatuor quadratorum. At numerator pluribus modis in quatuor quadrata resolvi potest; si enim ponatur

$$(aa+bb+cc+dd)(pp+qq+rr+ss)=xx+yy+zz+vv,$$

erit

$$\left.\begin{aligned} x&=ap+bq+cr+ds\\ y&=aq-bp\pm cs\mp dr\\ z&=ar\mp bs-cp\pm dq\\ v&=as\pm br\mp cq-dp \end{aligned}\right\}$$

qui quatuor numeri, si singuli dividantur per communem denominatorem $pp+qq+rr+ss$, dabunt radices quatuor quadratorum, quorum summa aequatur quoto proposito.

Nisi igitur hi numeri x, y, z et v sint divisibiles per $pp+qq+rr+ss$, saltem in fractis, assignari possunt quatuor quadrata, quorum summa aequalis est quoto $\frac{aa+bb+cc+dd}{pp+qq+rr+ss}$.

94. **Coroll. 1.** Quae hic de quatuor quadratorum summis sunt demonstrata, etiam ad summas trium, vel etiam duorum patent, cum nihil impediat, quominus unus, vel duo ex numeris a, b, c, d et p, q, r, s sint aequales nihilo.

94. **Coroll. 2.** Si igitur summa trium quadratorum per summam quatuor, vel etiam trium quadratorum dividatur, quotus certe erit summa quatuor quadratorum.

95. **Coroll. 3.** Quia productum ex duabus summis quatuor quadratorum est quoque summa quatuor quadratorum, patet, si omnes numeri primi sint summae quatuor quadratorum, vel etiam pauciorum, tum etiam omnes omnino numeros esse summas quatuor quadratorum, vel etiam pauciorum.

96. **Scholion.** Si summa quatuor quadratorum $aa + bb + cc + dd$ fuerit divisibilis per summam quatuor quadratorum $pp + qq + rr + ss$, tum quotum non solum in fractis, sed etiam in integris, esse summam quatuor quadratorum, est theorema elegantissimum Fermatii, cujus demonstratio cum ipso nobis est erepta. Fateor, me adhuc hanc demonstrationem invenire non potuisse, verumtamen hinc via aperitur ad theorema sequens demonstrandum, quo quilibet numerus summa quatuor quadratorum, vel pauciorum asseritur; casu scilicet, quo quadrata fracta non excluduntur: etsi enim hoc theorema in integris quoque semper verum sit, tamen non parum mihi praestitisse videor, quod id semota quadratorum integrorum ratione demonstraverim. Cum enim demonstratio adhuc post Fermatium sit frustra indagata, me proxime ad hunc scopum pertigisse arbitror.

97. **Theorema 20.** Omnis numerus est summa quatuor quadratorum, vel etiam pauciorum, siquidem quadrata fracta non excludantur.

Demonstratio. Theorema hoc quidem verum est, etiamsi quadrata fracta excludantur; Fermatius enim affirmat, omnem numerum integrum esse aggregatum ex quatuor quadratis integris, vel etiam paucioribus, ego autem fateor, me hanc demonstrationem nondum invenire potuisse; dabo ergo demonstrationem pro casu, quo quadrata fracta non excluduntur. Jam notavi hanc demonstrationem tantum ad numeros primos reduci, de quibus ergo sufficit theorema demonstrasse. Quoniam igitur novimus, numeros primos minores, ut 2, 3, 5, 7, 11, 13, etc., omnes in quatuor, vel pauciora quadrata resolvi posse, si quis id de sequentibus neget, ei dicendum est, dari aliquem numerum primum minimum, qui non sit summa quatuor pauciorumve quadratorum. Sit p iste numerus primus, ita ut omnes numeri primi ipso minores, hincque etiam omnes compositi certo sint summae quatuor pauciorumve quadratorum. Jam per theorema praecedens datur summa trium quadratorum, quae sit $aa + bb + cc$ divisibilis per numerum istum p, ita ut singula haec quadrata sint minora quam $\frac{1}{4}pp$; unde erit $aa + bb + cc < \frac{3}{4}pp$. Quotus ergo $\frac{aa + bb + cc}{p}$ erit minor, quam $\frac{3}{4}p$, qui cum idcirco minor sit, quam p, certe erit summa quatuor pauciorumve quadratorum; sit $xx + yy + zz + vv$ iste quotus, erit $p = \frac{aa + bb + cc}{xx + yy + zz + vv}$, ideoque ipse numerus p erit summa quatuor pauciorumve quadratorum, quae in fractionibus etiam assignari possunt. Cum igitur inter numeros primos non detur minimus, qui in quatuor vel pauciora quadrata dispertiri nequeat, nullus prorsus datur numerus primus, qui non esset aggregatum quatuor pauciorumve quadratorum, quod cum certum sit de numeris primis, etiam valebit de omnibus numeris compositis, ideoque de omnibus omnino numeris, ita ut nullus omnino detur numerus, qui non sit summa quatuor pauciorumve quadratorum.

98. **Coroll. 1.** Cum omnis numerus integer sit summa quatuor pauciorumve quadratorum, eadem proprietas etiam ad omnes numeros fractos patet. Sit enim proposita fractio quaecunque

$\frac{m}{n}$, quae transformetur in $\frac{mn}{nn}$. Jam sit $mn = \frac{aa}{pp} + \frac{bb}{qq} + \frac{cc}{rr} + \frac{dd}{ss}$, eritque

$$\frac{mn}{nn} = \frac{m}{n} = \frac{aa}{nnpp} + \frac{bb}{nnqq} + \frac{cc}{nnrr} + \frac{dd}{nnss};$$

ideoque omnis numerus fractus erit summa quatuor pauciorumve quadratorum.

99. **Coroll. 2.** Quoniam, si de resolutione numerorum fractorum in quadrata sermo est, conditio illa quadratorum integrorum sponte evanescit, theorema in latiori sensu ita acceptum, ut omnes plane numeros, sive integros, sive fractos, in quatuor vel pauciora quadrata resolubiles dicamus, sine ulla restrictione rigide demonstravi.

100. **Scholion.** Cum igitur Fermatius affirmasset, omnem numerum integrum esse summam vel quatuor vel pauciorum quadratorum integrorum: nunc quidem hoc est demonstratum de quadratis in genere spectatis, fractis non exclusis. Quare ut Fermatio satisfiat, superest ut demonstremus, qui numerus integer in quatuor quadrata fracta resolvi queat, eundem quoque in quatuor vel pauciora quadrata integra resolvi posse. In analysi quidem Diophantea pro certo assumi solet, nullum numerum integrum in quatuor quadrata fracta dispertiri posse, nisi ejus resolutio in quatuor quadrata integra vel pauciora constet: quod ergo si demonstratione esset confirmatum, nihil foret amplius desiderandum. Verum nusquam adhuc ejusmodi demonstrationem inveni. Quod autem ad theorema latissime patens attinet, his verbis conceptum:

Omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum,

ejus demonstrationem hic tradidi ita rigorosam, ut in ea nihil plane desiderari queat: hocque ipso non contemnendam partem demonstrationum Fermatianarum deperditarum mihi equidem videor restituisse.



XVI.

Demonstratio theorematis circa ordinem in summis divisorum observatum.

(N. Comment. V. 1754 — 55. p. 75.)

Jam ab aliquo tempore incidi in theorema, quo natura numerorum non mediocriter illustrari est visa, cum in eo ordo contineatur, quem summae divisorum, ex numeris serie naturali procedentibus ortae, inter se tenent. Ostendi enim, si singulorum numerorum naturalium 1, 2, 3, 4, 5, 6, 7, 8, etc. omnes divisores in unam summam colligantur, haecque divisorum summae in seriem disponantur, quae erit

1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28, 14, 24, 24, 31, 18, etc.

hanc seriem esse recurrentem, ejusque singulos terminos ex praecedentibus secundum quandam scalam relationis determinari. Atque hic ordo non solum ideo maxime notatu dignus est visus, quod vix quisquam suspicatus fuerit, hanc seriem certae cuipiam legi esse adstrictam, sed etiam, quod istius ordinis nullam demonstrationem firmam mihi quidem tum temporis reperire licuerit, etiamsi pluribus modis rem tentaverim. Perductus quidem fui ad hujus ordinis observationem, dum sequentem formulam in infinitum productam sum contemplatus:

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7) \text{ etc.}$$

ex cujus evolutione per inductionem conclusi fore

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + \text{etc.},$$

ubi exponentium ipsius x ordo eorum differentiis sumendis fit manifestus; erit enim series differentiarum 1, 1, 3, 2, 5, 3, 7, 4, 9, 5, 11, 6, 13, 7, 15, 8, etc. Excerptis enim terminis alternis patet, hanc seriem esse permixtam ex serie numerorum imparium, et ex serie numerorum omnium integrorum. Verum quod sit secundum hanc legem:

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \text{etc.}$$

siquidem fuerit

$$s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5) \text{ etc.}$$

per inductionem tantum collegi, neque aequalitatem harum duarum formularum solida demonstratione evincere potui. Quam ob causam etiam ordinem illum, quem in summis divisorum hinc elicui, firmiter demonstrare non valui; sed ejus demonstrationem jam tum inniti declaravi demonstrationi aequalitatis inter binas illas formulas infinitas modo exhibitas. Cum igitur nunc istam demonstrationem sim adeptus, ordinem quoque illum in summis divisorum detectum non amplius illis veritatibus, quae agnoscuntur, neque tamen demonstrari possunt, accenseri conveniet, quemadmodum tum temporis sum arbitratus, sed jam merito ipsi locus inter veritates rigide demonstratas assignari

poterit. Cujus rei ne ullum dubium relinquatur, singulas propositiones, quibus demonstratio hujus veritatis innititur, hic ordine apponam atque demonstrabo:

Propositio 1. Si sit $s = (1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)(1+\zeta)(1+\eta)$ etc. productum hoc, ex infinitis factoribus constans in seriem sequentem convertitur:

$$s = (1+\alpha) + \beta(1+\alpha) + \gamma(1+\alpha)(1+\beta) + \delta(1+\alpha)(1+\beta)(1+\gamma)$$
$$+ \varepsilon(1+\alpha)(1+\beta)(1+\gamma)(1+\delta) + \zeta(1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon) + \text{etc.}$$

Demonstratio. Cum enim seriei primus terminus sit $(1+\alpha)$ et secundus $= \beta(1+\alpha)$, erit summa primi et secundi $= (1+\alpha)(1+\beta)$: si jam addatur tertius terminus $\gamma(1+\alpha)(1+\beta)$, prodibit $(1+\alpha)(1+\beta)(1+\gamma)$: addatur insuper terminus quartus, qui est $\delta(1+\alpha)(1+\beta)(1+\gamma)$, erit summa $= (1+\alpha)(1+\beta)(1+\gamma)(1+\delta)$. Atque sic in infinitum procedendo, summa totius seriei, seu omnium ejus terminorum, perducetur ad hoc productum:

$$(1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)(1+\zeta) \text{ etc.}$$

Unde manifestum est, si fuerit

$$s = (1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)(1+\zeta) \text{ etc.}$$

fore vicissim:

$$s = (1+\alpha) + \beta(1+\alpha) + \gamma(1+\alpha)(1+\beta) + \delta(1+\alpha)(1+\beta)(1+\gamma) + \text{etc.}$$

Propositio 2. Si fuerit $s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)$ etc. productum hoc, ex infinitis factoribus constans, reducetur ad hanc seriem:

$$s = 1 - x - x^2(1-x) - x^3(1-x)(1-x^2) - x^4(1-x)(1-x^2)(1-x^3) - \text{etc.}$$

Demonstratio. Si haec forma $s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)$ etc. cum forma praecedente $s = (1+\alpha)(1+\beta)(1+\gamma)(1+\delta)(1+\varepsilon)$ etc. comparetur, manifestum est fore:

$$\alpha = -x, \quad \beta = -x^2, \quad \gamma = -x^3, \quad \delta = -x^4, \quad \varepsilon = -x^5, \text{ etc.}$$

His igitur valoribus in serie ibi data, quae producto s aequalis est inventa, rite substitutis, patebit propositionis veritas, scilicet esse:

$$s = 1 - x - x^2(1-x) - x^3(1-x)(1-x^2) - x^4(1-x)(1-x^2)(1-x^3) - \text{etc.}$$

Propositio 3. Si fuerit $s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)$ etc. erit hoc productum infinitum per multiplicationem evolvendo, terminosque secundum potestates ipsius x disponendo:

$$s = 1 - x^1 - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + x^{57} - \text{etc.},$$

cujus seriei ratio est ea ipsa, quae supra est exposita.

Demonstratio. Cum sit $s = (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)(1-x^6)(1-x^7)$ etc., erit $s = 1 - x - x^2(1-x) - x^3(1-x)(1-x^2) - x^4(1-x)(1-x^2)(1-x^3) - \text{etc.}$

Ponatur $s = 1 - x - Ax^2$, erit:

$$A = 1 - x + x(1-x)(1-x^2) + x^2(1-x)(1-x^2)(1-x^3) + \text{etc.}$$

Evolvantur singuli termini tantum secundum factorem $1-x$, ac sequenti modo disponantur:

$$A = \begin{cases} \quad -x \qquad\qquad -x^2(1-x^2) \qquad\qquad -x^3(1-x^2)(1-x^3) \qquad\qquad - \text{etc.} \\ +1 + x(1-x^2) + x^2(1-x^2)(1-x^3) + x^3(1-x^2)(1-x^3)(1-x^4) + \text{etc.} \end{cases}$$

eritque terminis subscriptis colligendis:

$$A = 1 - x^3 - x^5(1-x^2) - x^7(1-x^2)(1-x^3) - x^9(1-x^2)(1-x^3)(1-x^4) - \text{etc.}$$

Ponatur $A = 1 - x^3 - Bx^5$, erit

$$B = 1 - x^2 + x^2(1-x^2)(1-x^3) + x^4(1-x^2)(1-x^3)(1-x^4) + \text{etc.}$$

in quibus terminis subscriptis $1 - x^2$ tantum evolvatur, ac fiet

$$B = \begin{cases} \quad - x^2 \qquad - x^4(1-x^3) \qquad - x^6(1-x^3)(1-x^4) \qquad - \text{etc.} \\ 1 + x^2(1-x^3) + x^4(1-x^3)(1-x^4) + x^6(1-x^3)(1-x^4)(1-x^5) + \text{etc.} \end{cases}$$

denuoque terminis subscriptis colligendis habebitur:

$$B = 1 - x^5 - x^8(1-x^3) - x^{11}(1-x^3)(1-x^4) - x^{14}(1-x^3)(1-x^4)(1-x^5) - \text{etc.}$$

Ponatur $B = 1 - x^5 - Cx^8$, erit

$$C = 1 - x^3 + x^3(1-x^3)(1-x^4) + x^6(1-x^3)(1-x^4)(1-x^5) + \text{etc.},$$

ubi in singulis terminis factor $1 - x^3$ evolvatur, ut fiat scribendo ut supra:

$$C = \begin{cases} \quad - x^3 \qquad - x^6(1-x^4) \qquad - x^9(1-x^4)(1-x^5) \qquad - \text{etc.} \\ 1 + x^3(1-x^4) + x^6(1-x^4)(1-x^5) + x^9(1-x^4)(1-x^5)(1-x^6) + \text{etc.} \end{cases}$$

unde colligetur:

$$C = 1 - x^7 - x^{11}(1-x^4) - x^{15}(1-x^4)(1-x^5) - x^{19}(1-x^4)(1-x^5)(1-x^6) - \text{etc.}$$

Ponatur $C = 1 - x^7 - Dx^{11}$, erit

$$D = 1 - x^4 + x^4(1-x^4)(1-x^5) + x^8(1-x^4)(1-x^5)(1-x^6) + \text{etc.},$$

quae abit in hanc formam:

$$D = \begin{cases} \quad - x^4 \qquad - x^8(1-x^5) \qquad - x^{12}(1-x^5)(1-x^6) \qquad - \text{etc.} \\ 1 + x^4(1-x^5) + x^8(1-x^5)(1-x^6) + x^{12}(1-x^5)(1-x^6)(1-x^7) + \text{etc.} \end{cases}$$

sicque erit

$$D = 1 - x^9 - x^{14}(1-x^5) - x^{19}(1-x^5)(1-x^6) - x^{24}(1-x^5)(1-x^6)(1-x^7) - \text{etc.}$$

Quodsi porro ponatur $D = 1 - x^9 - Ex^{14}$, reperietur simili modo:

$$E = 1 - x^{11} - Fx^{17};$$

hincque ultra:

$$F = 1 - x^{13} - Gx^{20}, \quad G = 1 - x^{15} - Hx^{23}, \quad H = 1 - x^{17} - Jx^{26}, \text{ etc.}$$

Restituamus jam sucessive hos valores, eritque:

$$\begin{aligned} s &= 1 - x - Ax^2 \\ Ax^2 &= x^2(1-x^3) - Bx^7 \\ Bx^7 &= x^7(1-x^5) - Cx^{15} \\ Cx^{15} &= x^{15}(1-x^7) - Dx^{26} \\ Dx^{26} &= x^{26}(1-x^9) - Ex^{40} \text{ etc.} \end{aligned}$$

Quamobrem habebimus:

$$s = 1 - x - x^2(1 - x^3) + x^7(1 - x^5) - x^{15}(1 - x^7) + x^{26}(1 - x^9) - x^{40}(1 - x^{11}) + \text{etc.}$$

sive id ipsum, quod demonstrari oportet:

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + \text{etc.}$$

unde simul lex exponentium supra indicata per differentias luculenter perspicitur.

Propositio 4., seu Theorema principale demonstrandum. Si haec scribendi formula $\int n$ denotet summam omnium divisorum numeri n, similique modo summae divisorum numerorum minorum, veluti $n - a$, designentur per $\int(n-a)$, summa divisorum numeri n, seu $\int n$ ita pendebit a summis divisorum numerorum minorum, ut sit

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) - \int(n-22)$$
$$- \int(n-26) + \int(n-35) + \int(n-40) - \int(n-51) - \int(n-57) + \text{etc.}$$

Ubi sequentia sunt notanda:

1. Signa $+$ et $-$ geminata terminos hujus progressionis alternatim afficere.

2. Legem numerorum 1, 2, 5, 7, 12, 15, 22, 26, etc. ex eorum differentiis, quae sunt 1, 3, 2, 5, 3, 7, 4, etc. fieri manifestam; unde colligitur hos numeros omnes in formula hac generali $\frac{3zz \pm z}{2}$ contineri.

3. Quovis casu istius progressionis eos tantum terminos ab initio esse accipiendos, qui post signum $\int$ numeros affirmativos retineant; reliquos vero omnes, quibus signum $\int$ numeris negativis praefigitur, esse omittendos; ita si sit $n = 10$, erit

$$\int 10 = \int 9 + \int 8 - \int 5 - \int 3 = 13 + 15 - 6 - 4 = 18.$$

4. Quibus casibus occurrit terminus $\int(n-n)$, quod evenit, si n fuerit numerus hujus seriei 1, 2, 5, 7, 12, 15, etc. iis casibus pro valore hujus termini $\int(n-n)$, seu $\int 0$ assumi oportere ipsum numerum propositum n; sic si sit $n = 7$, erit

$$\int 7 = \int 6 + \int 5 - \int 2 - \int 0 = 12 + 6 - 3 - 7 = 8,$$

et si sit $n = 12$, erit

$$\int 12 = \int 11 + \int 10 - \int 7 - \int 5 + \int 0 = 12 + 18 - 8 - 6 + 12 = 28.$$

Demonstratio. Formetur series $z = x\int 1 + x^2\int 2 + x^3\int 3 + x^4\int 4 + x^5\int 5 + \text{etc.}$, ubi quaelibet potestas ipsius x multiplicata sit per summam divisorum exponentis ejus potestatis. Quodsi jam singulae divisorum summae resolvantur, manifestum est, hanc seriem transformari in hanc formam

$$z = 1(x + x^2 + x^3 + x^4 + x^5 + \text{etc.}) + 2(x^2 + x^4 + x^6 + x^8 + x^{10} + \text{etc.})$$
$$+ 3(x^3 + x^6 + x^9 + x^{12} + x^{15} + \text{etc.}) + 4(x^4 + x^8 + x^{12} + x^{16} + x^{20} + \text{etc.})$$
$$+ 5(x^5 + x^{10} + x^{15} + x^{20} + x^{25} + \text{etc.}) + 6(x^6 + x^{12} + x^{18} + x^{24} + x^{30} + \text{etc.}) + \text{etc.}$$

quibus seriebus geometricis summatis fiet:

$$z = \frac{1x}{1-x} + \frac{2xx}{1-xx} + \frac{3x^3}{1-x^3} + \frac{4x^4}{1-x^4} + \frac{5x^5}{1-x^5} + \frac{6x^6}{1-x^6} + \text{etc.}$$

Multiplicetur haec forma per $-\frac{dx}{x}$, ac producti integrale erit

$$-\int \frac{z\,dx}{x} = l(1-x) + l(1-xx) + l(1-x^3) + l(1-x^4) + l(1-x^5) + \text{etc.}$$

seu $$-\int\frac{z\,dz}{x} = l\,(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)\ \text{etc.}$$

quae expressio post signum logarithmicum, cum sit eadem, quae in propositione praecedente vocata est $= s$, erit $-\int\frac{z\,dx}{x} = ls$, ideoque alterum valorem pro s sumendo, erit quoque:

$$-\int\frac{z\,dx}{x} = l\,(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - \text{etc.}),$$

cujus differentiale per $\frac{-dx}{x}$ divisum, dabit alium valorem pro z, nempe

$$z = \frac{1x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - 22x^{22} - \text{etc.}}{1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + \text{etc.}}$$

qui valor si aequalis ponatur assumto, et utrinque per denominatorem $1 - x - x^2 + x^5 + x^7 - x^{12} - \text{etc.}$ multiplicetur, reperietur terminis secundum potestates ipsius x disponendis, omnibusque ad eandem partem collocandis:

$$\begin{array}{rcccccccccc}
0 = & x\int 1 & + x^2\int 2 & + x^3\int 3 & + x^4\int 4 & + x^5\int 5 & + x^6\int 6 & + x^7\int 7 & + x^8\int 8 & + x^9\int 9 & + x^{10}\int 10 + \text{etc.} \\
 & . & -\int 1 & -\int 2 & -\int 3 & -\int 4 & -\int 5 & -\int 6 & -\int 7 & -\int 8 & -\int 9 \\
 & . & . & -\int 1 & -\int 2 & -\int 3 & -\int 4 & -\int 5 & -\int 6 & -\int 7 & -\int 8 \\
 & . & . & . & . & . & +\int 1 & +\int 2 & +\int 3 & +\int 4 & +\int 5 \\
 & . & . & . & . & . & . & . & +\int 1 & +\int 2 & +\int 3 \\
 & . & . & . & . & . & . & . & . & . & . \\
 & -1 & -2 & * & * & +5 & * & +7 & * & * & *
\end{array}$$

unde singularum potestatum ipsius x coefficientibus nihilo aequatis, sequitur fore

$$\begin{array}{ll}
\int 1 = 1 & \int 6 = \int 5 + \int 4 - \int 1 \\
\int 2 = \int 1 + 2 & \int 7 = \int 6 + \int 5 - \int 2 - 7 \\
\int 3 = \int 2 + \int 1 & \int 8 = \int 7 + \int 6 - \int 3 - \int 1 \\
\int 4 = \int 3 + \int 2 & \int 9 = \int 8 + \int 7 - \int 4 - \int 2 \\
\int 5 = \int 4 + \int 3 - 5 & \int 10 = \int 9 + \int 8 - \int 5 - \int 3
\end{array}$$

atque indolem illius aequationis vel leviter attendenti patebit, esse generatim:

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \int(n-12) + \int(n-15) - \text{etc.}$$

hac progressione quovis casu eousque continuata, donec perveniatur ad summas numerorum negativorum. Deinde per se est perspicuum, numeros absolutos 1, 2, 5, 7, etc., qui in illis formulis conspiciuntur, vicem tenere termini $\int 0$; unde concluditur, in casibus quibus pro $\int n$ in progressione illa reperta occurrit terminus $\int(n-n)$, seu $\int 0$, valorem ejus semper ipsi numero proposito n aequalem esse capiendum: sicque habetur plena ac perfecta demonstratio theorematis propositi, quae, cum praeter tractationem serierum infinitarum, per logarithmos et differentialia procedat, minus quidem naturalis, sed ob hoc ipsum multo magis notabilis est aestimanda.

XVII.

Solutio problematis de investigatione trium numerorum, quorum tam summa, quam productum, nec non summa productorum ex binis, sint numeri quadrati.

(N. Comment. VIII. 1760—61. p. 64. Exhib. 1756. Mart. 8.)

1. Etsi problemata hujus generis, quae Diophantea appellari solent, parum utilitatis afferre videntur: tamen certum est, analysin mathematicam, atque adeo etiam eam partem, quae circa infinita versatur, ex methodo problemata Diophantea solvendi, maxima incrementa cepisse. Non solum autem hujusmodi problemata, si sint difficiliora, fines analyseos plurimum amplicaverunt: sed etiam vim ingenii mirifice acuere solent, ut etiam in aliis problematibus, quomodo solutionem institui oporteat, facilius perspicere valeat. Quam ob rem hujus generis problemata, praecipue si modus solvendi magis fuerit reconditus, minime contemnenda esse arbitror. Dum enim singularia artificia ad eorum solutionem requiruntur, ab iisdem quoque egregia subsidia ad universam analysin uberius excolendam expectare licebit.

2. Ad hoc autem genus potissimum referendum videtur problema propositum, quandoquidem id diu et multum per varia methodi Diophanteae artificia frustra tractavi, ut fere etiam de ejus solutione penitus desperaverim. Tandem vero, quasi inopinato, solutionem sum consecutus, quae eo magis notatu digna videbatur, quod minimi numeri, quos quidem adhuc satisfacientes elicere potui, sunt ita praegrandes, ut mirum non sit, solutionem tantis difficultatibus fuisse involutam. Quare cum methodo singulari ad istam solutionem pertigerim, ejus ampliorem explicationem usu non esse carituram arbitror, cum simili fortasse modo aliae quaestiones multo adhuc difficiliores superari queant.

3. Quaerantur ergo tres numeri, quibus tres sequentes conditiones conveniant:

I. Ut eorum summa sit numerus quadratus.

II. Ut summa productorum ex binis sit numerus quadratus.

III. Ut productum omnium trium sit numerus quadratus.

Quod problema etiam hoc modo enunciari potest, ut quaeratur aequatio $z^3 - pzz + qz - r = 0$, omnes suas radices habens rationales, cujus singuli coefficientes p, q et r sint numeri quadrati. Posset adhuc adjici haec conditio, ut isti numeri sint integri; verum per se est perspicuum, quomodo inventis ternis numeris fractis satisfacientibus, ex iis facile integri, qui etiam satisfaciant, formari queant. Quicunque enim terni numeri satisfacere fuerint inventi, iidem per numerum quadratum quemcunque multiplicati aeque satisfacient, quo pacto fractiones facillime tollentur.

4. Sint igitur nx, ny, nz tres hujusmodi numeri quaesiti, ac satisfieri oportebit his conditionibus:

I. Ut sit $n(x+y+z) =$ quadrato.

II. Ut sit $nn(xy+xz+yz)$, seu $xy+xz+yz =$ quadrato.

III. Ut sit n^3xyz, seu $nxyz =$ quadrato.

At primae et tertiae conditioni satisfiet, si reddatur

$$xyz(x+y+z) = \text{quadrato}.$$

Ponatur ergo: $$xyz(x+y+z) = vv(x+y+z)^2,$$

unde per $x+y+z$ dividendo erit

$$xyz = vv(x+y+z), \quad \text{hincque} \quad z = \frac{vv(x+y)}{xy-vv}.$$

Cum igitur hinc fiat $xyz = \frac{vvxy(x+y)}{xy-vv}$, ut $nxyz$ prodeat quadratum, capi debet

$$n = m^2xy(x+y)(xy-vv).$$

Hisque valoribus pro z et n assumtis, satisfactum erit primae et tertiae conditioni.

5. Hinc itaque nostri tres numeri erunt

primus $nx = mmxxy(x+y)(xy-vv)$,

secundus $ny = mmxyy(x+y)(xy-vv)$,

tertius $nz = mmvvxy(x+y)^2$,

ubi per numerum arbitrarium m fractiones, si quae forte occurrent, tolli poterunt. Verum contemplemur jam secundam conditionem, quae ob $z = \frac{vv(x+y)}{xy-vv}$ requirit, ut sit:

$$xy + \frac{vv(x+y)^2}{xy-vv} = \text{quadrato}.$$

Ponamus in hunc finem:

$$xy - vv = uu, \quad \text{ut sit} \quad y = \frac{vv+uu}{x} \quad \text{et} \quad z = \frac{vv(x+y)}{uu},$$

erit $xy = vv+uu$ et $x+y = \frac{xx+vv+uu}{x}$, efficiendumque est, ut sit

$$vv + uu + \frac{vv(xx+vv+uu)^2}{uuxx} = \text{quadrato}.$$

6. Ponatur $x = tv$; ut sit $y = \frac{vv+uu}{tv}$, esseque debet

$$vv + uu + \frac{(vv(tt+1)+uu)^2}{ttuu} = \text{quadrato},$$

seu multiplicando per $ttuu$

$$ttuuvv + ttu^4 + v^4(tt+1)^2 + 2uuvv(tt+1) + u^4 = \text{quadrato},$$

sive $$v^4(tt+1)^2 + uuvv(3tt+2) + u^4(tt+1) = \text{quadrato}.$$

Statuatur hujus quadrati radix $= vv(tt+1) + suu$, erit

$$vv(3tt+2) + uu(tt+1) = 2svv(tt+1) + ssuu;$$

unde elicitur $$\frac{vv}{uu} = \frac{tt+1-ss}{2s(tt+1)-3tt-2} = \text{quadrato}.$$

Sit porro $s = t - r$, et habebitur:

$$\frac{vv}{uu} = \frac{2rt - rr + 1}{2t^3 - (2r+3)tt + 2t - 2(r+1)}.$$

Multiplicetur numerator et denominator per $2rt - rr + 1$, ut fiat

$$\frac{vv}{uu} = \frac{(2rt - rr + 1)^2}{4rt^4 - 2(3rr + 3r - 1)t^3 + (2r^3 + 3rr + 2r - 3)tt - 2(3r - 1)(r + 1)t + 2(r - 1)(r + 1)^2}.$$

7. Tota ergo quaestio huc est perducta, ut hujus fractionis denominator reddatur quadratum: posito enim

$$4rt^4 - 2(3rr + 3r - 1)t^3 + (2r^3 + 3rr + 2r - 3)tt - 2(3r - 1)(r + 1)t + 2(r - 1)(r + 1)^2 = QQ,$$

erit definitis hinc t et r

$$\frac{v}{u} = \frac{2rt - rr + 1}{Q}, \quad \text{tum vero} \quad x = tv \quad \text{et} \quad y = \frac{vv + uu}{tv}$$

unde numeri quaesiti definientur. Ante autem, quam ad istam aequationem pertigimus, solutionem jam limitavimus positione $xy - vv = uu$, quae restrictio probe est notanda, quoniam nullum est dubium, quin ejusmodi extent solutiones, in quibus $xy - vv$ non sit numerus quadratus, easque propterea hinc non reperiemus. Verum hanc limitationem ideo facere sum coactus, ut ad istam formulam quadrato aequandam pervenire licuerit, quippe quae ita est comparata, ut per cognita artificia resolvi possit. Sicque tota solutionis vis in reductionibus § praeced. est sita.

8. Pluribus autem casibus haec formula et quidem infinitis modis quadratum effici potest, quorum praecipui, et qui statim se offerunt, sunt: 1) si coefficiens ipsius t^4, scilicet $4r$, seu r, fuerit numerus quadratus; 2) si terminus ultimus $2(r - 1)(r + 1)^2$ seu $2(r - 1)$ fuerit numerus quadratus: utroque enim casu per regulas cognitas valores idonei pro t elici, tum vero porro ex quolibet alii novi inveniri possunt. Sin autem simul et r et $2(r - 1)$ fuerint quadrata, una operatione plures valores idoneos pro t eruere licet, neque vero hic, ut plerumque fieri solet, solutio simplicior se offert; etsi enim si $2(r - 1) =$ quadrato, satisfacit valor $t = 0$, tamen inde prodit $x = 0$ et $y = \infty$, qui valores pro natura quaestionis plane sunt incongrui. Excluduntur enim solutiones, quibus unus trium numerorum quaesitorum evanesceret, quia tum quaestio esset facillima et circa duos numeros versaretur, quorum tam summa, quam productum, esset quadratum.

9. **Casus I.**, quo ponitur $r = 1$. Hic casus simplicissimus videtur, quia ultimus terminus nostrae formae evanescit, primusque fit quadratus. Habemus ergo

$$4t^4 - 10t^3 + 4tt - 8t = QQ \quad \text{et} \quad \frac{v}{u} = \frac{2t}{Q}.$$

Ad hanc aequationem solvendam statuamus $Q = 2tt - \frac{5}{2}t$ eritque

$$4tt - 8t = \frac{25}{4}tt, \quad \frac{9}{4}t = -8 \quad \text{et} \quad t = -\frac{32}{9}.$$

At hinc fiet $\frac{v}{u} = \frac{4}{4t - 5} = \frac{-36}{173}$; unde habebimus

$$v = -36, \quad u = 173, \quad t = \frac{-32}{9} \quad \text{et} \quad x = tv = 128$$

indeque porro $$y = \frac{36^2 + 173^2}{128} = \frac{31225}{128} = \frac{25.1249}{128}.$$

Erit ergo $$x + y = \frac{47609}{128} \quad \text{et} \quad z = \frac{36^2.47609}{173^2.128}$$

ac tres numeri quaesiti erunt, ob $xy - vv = uu$,

$$\text{Primus} = \frac{128^2 . 25 . 1249 . 47609 . 173^2}{128 . 128} mm$$

$$\text{Secundus} = \frac{128 . 25^2 . 1249^2 . 47609 . 173^2}{128^2 . 128} mm$$

$$\text{Tertius} = \frac{36^2 . 128 . 25 . 1249 . 47609^2}{128 . 128^2} mm.$$

10. Ad fractiones tollendas ponamus $m = \frac{128}{5}$, eruntque terni nostri numeri

$$\left.\begin{array}{ll} \text{Primus} = 128^2 . 173^2 . 1249 . 47609 & = 128^2 . 173^2 \\ \text{Secundus} = 5^2 . 173^2 . 1249^2 . 47609 & = 5^2 . 173^2 . 1249 \\ \text{Tertius} = 36^2 . 1249 . 47609^2 & = 36^2 . 47609 \end{array}\right\} \text{in } 1249 . 47609,$$

quibus numeris evolutis erit

$$\begin{array}{ll} \text{Primus} & = 490356736 . 59463641 \\ \text{Secundus} & = 934533025 . 59463641 \\ \text{Tertius} & = 61701264 . 59463641 \end{array}$$

quorum productum manifesto est quadratum, quippe

$$5^2 . 36^2 . 128^2 . 173^4 . 1249^4 . 47609^4.$$

Summa autem reperitur $25 . 59463641^2$

et summa productorum ex binis $173^2 . 59463641^2 . 18248924559376$

cujus radix quadrata est $173 . 59463641 . 4271876$

11. Pro eadem aequatione resolvenda poni potest $Q = 2tt - \frac{5}{2}t - \frac{9}{16}$, ut tres priores termini tollantur, ac prodibit

$$-8t = +\frac{45}{16}t + \frac{81}{256}, \text{ seu } 0 = 173t + \frac{81}{16}, \text{ ergo } t = \frac{-81}{16.173}.$$

$$\text{Hinc } Q = \frac{81^2}{128.173^2} + \frac{405}{32.173} - \frac{9}{16} = -\frac{9.207563}{128.173^2} \text{ et } \frac{v}{u} = \pm\frac{144.173}{207563}.$$

Sumi enim potest valor ipsius Q tam negative quam positive. Statuatur ergo

$$v = -144.173, \quad u = 207563, \quad \text{erit} \quad x = 9 . 81 = 729 \quad \text{et} \quad y = \frac{vv + uu}{729};$$

unde jam manifestum est, ad tam enormes perveniri numeros, ut solutio praecedens prae hac multo simplicior sit aestimanda. Superfluum autem foret, hujusmodi solutiones nimis complicatas ulterius evolvere, quia in hujus generis quaestionibus solutione simplicissima plerumque contenti esse solemus.

12. **Casus 2.**, quo ponitur $r = \frac{1}{2}$. Hac positione ultimus formulae nostrae terminus fit quadratum, eritque $\frac{v}{u} = \frac{12t - 5}{4Q}$, existente

$$QQ = 6t^4 - \frac{41}{2}t^3 + \frac{27}{2}tt - \frac{35}{2}t + \frac{25}{4}.$$

Jam ad tres terminos ultimos tollendos, statuatur

$$Q = \frac{5}{2} - \frac{7}{2}t + \frac{1}{4}tt, \quad \text{eritque} \quad 6t^4 - \frac{41}{2}t^3 = \frac{1}{16}t^4 - \frac{7}{4}t^3 \quad \text{et} \quad t = \frac{60}{19}.$$

Hincque $Q = \frac{4357}{722}$ et $\frac{v}{u} = \frac{19}{14}$, unde $v = 19$ et $u = 14$. Nunc igitur erit $x = tv = 60$, et $y = \frac{vv + uu}{x} = \frac{557}{60}$, ideoque $x + y = \frac{4157}{60}$ et tres numeri quaesiti:

$$\text{Primus} = \frac{60^2.557\ 4157.196}{60.60} mm = 14^2.60^2.557.4157$$

$$\text{Secundus} = \frac{60.557^2.4157.196}{60.60.60} mm = 14^2.557^2.4157$$

$$\text{Tertius} = \frac{361.60.557.4157^2}{60.60.60} mm = 19^2.557.4157^2$$

posito $m = 60$: hique numeri jam notabiliter sunt minores quam ii, qui casu primo sunt inventi.

13. Quoniam ergo hi numeri ob parvitatem attentione digni videntur, ii ita exhibeantur:

$$\text{Primus} = 705600.2315449$$
$$\text{Secundus} = 109172.2315449$$
$$\text{Tertius} = 1500677.2315449.$$

Quorum numerorum summa est $= 2315449^2$, et productum $= 14^4.19^2.60^2.557^4.4157^4$, sicque uterque numerus quadratus.

At summa productorum ex binis erit

$$(14^2.60^2.14^2.557 + 14^2.60^2.19^2.4157 + 14^2.557.19^2.4157)\,2315449^2,$$

quae reducitur ad hanc formam: $14^2.2315449^2.6631333489$

cujus radix quadrata est $14.2315449.81433.$

Sunt autem hi numeri circiter 15000 vicibus minores, quam primum inventi.

14. **Casus 3.,** quo ponitur $r = 3$. Posito $r = 3$, fit $\frac{v}{u} = \frac{6t-8}{Q}$, et habebitur haec aequatio resolvenda: $QQ = 12t^4 - 70t^3 + 84tt - 64t + 64.$

Jam ad ternos ultimos terminos tollendos statuatur

$$Q = 8 - 4t + \frac{17}{4}tt, \quad \text{eritque} \quad 12t^4 - 70t^3 = \frac{289}{16}t^4 - 34t^3$$

unde elicitur $t = -\frac{576}{97}$ et $Q = \pm\frac{8.213601}{97.97}.$

Ergo $\frac{v}{u} = -\frac{97.529}{213601} = -\frac{97.23}{9287} = -\frac{23.97}{37.251}.$

ideoque $v = -23.97$ et $u = 37.251$: tum $x = tv = 23.24^2$ et $y = \frac{91225730}{23.24^2}.$

Verum facile perspicitur, hos numeros in immensum excrescere, unde iis evolvendis supersedemus. Contemplemur ergo adhuc unum casum, quo tam primus, quam ultimus terminus formulae QQ fiunt quadrati.

15. **Casus 4.,** quo ponitur $r = 9$. Posito $r = 9$, fit $\frac{v}{u} = \frac{18t-80}{Q}$, existente

$$QQ = 36t^4 - 538t^3 + 1716tt - 520t + 1600.$$

Tollamus terminos primum et duos ultimos, ponendo $Q = 40 - \frac{13}{2}t \pm 6tt$, et habebimus

$$-538t^3 + 1716tt = \mp 78t^3 \pm 480tt + \frac{169}{4}tt$$

unde elicimus pro utroque signo:

$$\left.\begin{array}{ll}\text{superiori} & t = \frac{5.191}{16.23} \\ \text{inferiori} & t = \frac{5.1723}{32.77}\end{array}\right\} \text{utrinque autem prodeunt numeri nimis magni.}$$

Tollamus ergo tres terminos ultimos, ponendo

$$Q = 40 - \frac{13}{2}t + \frac{1339}{64}tt;$$

hinc autem numeri multo adhuc majores resultant. Posset porro pro binis terminis primis cum ultimo tollendis poni $Q = 6tt - \frac{269}{6}t \pm 40$, verum hinc multo minus ad numeros simpliciores perveniemus.

16. Ex his satis tuto concludi posse videtur, minimos numeros problemati satisfacientes esse eos, quos § 13 elicuimus, qui ergo, si penitus per multiplicationem evolvantur, erunt:

Primus = 1633780814400.
Secundus = 252782198228.
Tertius = 3474741058973.

Sin autem in fractionibus numeri satisfacientes simplicissimi desiderentur, ii indidem assignari poterunt, his per 2315449^2 dividendis: ita ut hi numeri futuri sint:

$$\text{Primus} = \frac{705600}{2315449},$$

$$\text{Secundus} = \frac{196}{4157},$$

$$\text{Tertius} = \frac{361}{557}.$$

Quorum tam summa, quam summa productorum ex binis, et omnium trium productum, sunt numeri quadrati.



XVIII.

De problematibus indeterminatis, quae videntur plus quam determinata.

(N. Comment. VI. 1756—57. p. 85.)

Omnia problemata, quae in analysi Diophantea proponi solent, esse indeterminata, vel ipsa rei natura declarat; etsi enim plures ejusmodi quaestiones occurrant, quae non nisi unicam solutionem admittunt, veluti si quaeratur cubus, qui unitate auctus faciat quadratum, cui quaestioni praeter cubum 8 alius nullus satisfacere reperitur; tamen ne tales quidem quaestiones ad problemata determinata referri convenit, propterea quod methodus eas resolvendi tota ex ratione problematum indeterminatorum est petita, atque casui potissimum singulari tribuendum videtur, si unica solutio tantum locum habeat. Quemadmodum etiam non desunt ejusmodi quaestiones, quae plane nullam solutionem admittunt, quae tamen nihilo minus quaestionibus indeterminatis recte annumerantur: ante enim quam certiores fuerimus facti, nullam dari solutionem, id quod operatio ususque methodorum demum declarat, eas pro indeterminatis omnino habere debemus, nostramque investigationem perinde adornare, ac si infinita solutionum multitudo daretur. Ita si quaeri debeant tria quadrata, quorum summa faciat 7, nemo dubitabit, quin haec quaestio indeterminatis sit accensenda, etiamsi deinceps investigatione peracta impossibilitas solutionis manifesto se prodat. Quando igitur hic de problematibus indeterminatis tractare constitui, quae plus quam determinata videantur; ne quis putet haec invicem pugnare, fierique non posse, ut quod indeterminatum sit, idem plus quam determinatum videri queat, instituti rationem clarius exponi oportere sentio. Ac primo quidem nullum est dubium, quin cuilibet quaestioni Diophanteae ejusmodi insuper conditiones adjici queant, quibus ea non tam determinata, quam impossibilis reddatur. Veluti si quaestioni, qua duo quadrata petuntur, quorum summa sit quadratum, insuper haec conditio adjiciatur, ut eorundem quadratorum differentia quoque sit quadratum, quaestio, quae primum erat maxime indeterminata, hac unica conditione adjuncta fit impossibilis, ideoque merito pro plus quam determinata habetur. Simili modo tria quadrata quaerere in progressione arithmetica, problema est indeterminatum et innumerabiles solutiones admittens, statim vero ac quatuor quadrata in arithmetica progressione requiruntur, problema non determinatur, sed prorsus fit impossibile et plus quam determinatum.

Ex his exemplis manifestum est quaestionem indeterminatam per additionem unicae conditionis reddi posse plus quam determinatam, ideoque impossibilem. E contrario vero dantur ejusmodi quoque quaestiones, quae jam tot conditiones continent, ut unica nova conditione super addita, pari jure, ac commemoratae, plus quam determinatae fieri debere videantur, quibus tamen nihilo minus non una, sed plures saepe conditiones adjungi possunt, ita ut iis non obstantibus infinitae adhuc solutiones exhiberi queant; cujusmodi casus ex hoc problemate clarissime intelligetur.

Quaerantur tres numeri, ut binorum productum addito tertio fiat quadratum.

Scilicet vocando hos tres numeros x, y, z, requiritur ut sit:

$$xy + z = \text{quadr.}, \quad xz + y = \text{quadr.}, \quad yz + x = \text{quadr.}$$

Haec quaestio tentanti, nisi singularia artificia adhibeantur, jam solutu tam difficilis apparebit, ut si nova conditio super adderetur, de solutione plane sit desperaturus. Si enim ponat $xy + z = aa$, ut habeat $z = aa - xy$, ambae reliquae formulae quadratum efficiendae erunt:

$$aax - xxy + y \quad \text{et} \quad aay - xyy + x,$$

quarum priorem si ponat $= bb$, habebit quidem $y = \frac{aax - bb}{xx - 1}$, at hoc valore in tertia substituto, quadratum reddi debebit haec expressio:

$$x^5 - 2x^3 + aabbxx - (a^4 + b^4 - 1)x + aabb$$

quae certe jam est tam complicata, ut omnem solutoris sollertiam requirat, neque de novis conditionibus insuper adimplendis sit cogitandum.

Interim tamen huic quaestioni has insuper conditiones adjicere licet, ut binorum numerorum productum cum eorundem summa quoque faciat quadratum, seu ut sit:

$$xy + x + y = \square, \quad xz + x + z = \square, \quad yz + y + z = \square.$$

Quis igitur non putaret, his tribus conditionibus adjectis, problema propositum, jam per se satis difficile, fieri plus quam determinatum? Interim tamen certum est, et hoc casu problema adhuc esse indeterminatum, atque adeo in numeris integris infinitas solutiones admittere.

Quin etiam insuper hae conditiones adjici possunt, manente solutionum numero, et quidem in numeris integris, infinito: 1) ut summa productorum ex binis sit quadratum, 2) ut eadem summa productorum ex binis una cum ipsorum numerorum summa fiat quadratum.

Nec vero nunc quidem conditionum multitudo exhausta est censenda; nam postulari insuper potest, ut trium quaesitorum numerorum vel unus, vel adeo duo, sint ipsi quadrati, et quidem integri. Quodsi autem omnes tres debeant esse quadrati, ne nunc quidem problema fit plus quam determinatum, sed infinitas adhuc solutiones, etsi non in numeris integris, admittit; ac fortasse adhuc plures conditiones addi possent, quibus quoque satisfieri liceret.

En ergo problema, quod merito cuique plus quam determinatum videri debet.

Invenire tres numeros integros x, y, z, ut sequentes formulae omnes fiant quadrata:

$$\begin{array}{lll} xy + z = \square, & xy + x + y = \square, & xy + xz + yz = \square, \\ xz + y = \square, & xz + x + z = \square, & xy + xz + yz + x + y + z = \square, \\ yz + x = \square, & yz + y + z = \square, & \end{array}$$

cujus simplicissima solutio sine dubio est:

$$x = 1, \quad y = 4 \quad \text{et} \quad z = 12$$

tum vero etiam sequentes solutiones in promptu sunt:

$$\begin{array}{llllll} x = 1, & x = 4, & x = 4, & x = 1, & x = 1, & x = 4, \\ y = 12, & y = 9, & y = 12, & y = 24, & y = 40, & y = 33, \\ z = 24, & z = 28, & z = 33, & z = 40, & z = 60, & z = 64. \end{array}$$

Verum si haec conditio insuper sit adjecta, ut ipsi tres numeri quaesiti debeant esse quadrati, in fractis ecce has solutiones:

$$x=\frac{9}{64},\quad x=\frac{49}{64},\quad x=\frac{25}{9},\quad x=\frac{9}{25},$$
$$y=\frac{25}{64},\quad y=\frac{225}{64},\quad y=\frac{64}{9},\quad y=\frac{64}{25},$$
$$z=\frac{49}{16},\quad z=\frac{169}{16},\quad z=\frac{196}{9},\quad z=\frac{196}{25}.$$

Hujusmodi autem quaestio, inquam, merito pro plus quam determinata habetur, has enim conditiones non pro arbitrio adjecimus, atque in ipsa indagatione hujusmodi conditionum, quas indoles problematis patitur, praecipua pars artificii continetur. Namque si quis ad arbitrium conditiones superaddere vellet, admodum probabile esset, problema, vel unica adjecta, re vera fieri plus quam determinatum; quam ob rem talia problemata, tot conditionibus onerata, recte statim tanquam plus quam determinata spectantur, nisi aliunde constet, conditiones eas ab insigni artifice esse adjectas.

Talia problemata autem jam in ipso Diophanto occurrunt, quae commentatoribus non parum negotii fecerunt, cum quaedam tantum conditiones calculum tantopere occupent, ut reliquarum ratio neutiquam haberi posse videatur. Praemittuntur autem ejusmodi problematibus certae quaedam propositiones, quae ibi Porismata vocantur, in quibus tota solutionis vis continetur. Ostenditur scilicet, si quibusdam conditionibus certo quodam modo satisfiat, tum simul aliis quoque conditionibus quasi sponte satisfieri, ita ut non opus sit calculum seorsim ad eas applicare. Ita pro quaestione exempli loco allegata, qua tres numeri x, y et z quaeruntur, ut conditiones praescriptae impleantur, porisma praemittendum ita se habet:

Si quaerantur duo numeri x *et* y, *ut* $xy+x+y$ *fiat quadratum, puta* $=uu$, *atque tertius numerus* z *ita capiatur, ut sit* $z=1+x+y\pm 2u$, *tum non solum hae formulae*

$$xz+x+z \quad et \quad yz+y+z \quad \textit{fient quadrata:}$$

sed etiam hae $\quad xy+z,\quad xz+y \quad et \quad yz+x$

una cum istis $\quad xy+xz+yz \quad et \quad xy+xz+yz+x+y+z$

sponte fient quadrata.

Cum igitur huic unicae conditioni, qua formula $xy+x+y$ quadratum reddi debet, facillime satisfiat, ope hujus porismatis quaestio tam multis conditionibus circumscripta, ut plus quam determinata videatur, nullo plane labore infinitis modis resolvitur, et quidem in numeris integris.

Ponatur enim $xy+x+y=uu$, et cum sit $xy+x+y+1=(x+1)(y+1)=uu+1$ pro uu tale sumatur quadratum, quod unitate auctum habeat factores; sit scilicet $uu+1=mn$, et numeri problemati satisfacientes erunt: $x=m-1$, $y=n-1$ et $z=m+n-1\pm 2u$. In hujusmodi igitur problematibus totum negotium vertitur in inventione idoneorum illorum porismatum, quibus tota solutio ita contineatur, ut statim atque aliquibus conditionibus satisfecerimus, simul reliquas adimpleverimus. Cum igitur ratio talium porismatum a nemine adhuc sit explicata, si eam accuratius exposuero, non exiguum incrementum universa analysis Diophantea inde accepisse erit existimanda. Tota autem horum porismatum ratio sequenti lemmati per se perspicuo inniti videtur.

1. **Lemma.** *Si inventi fuerint valores litterarum* z, y, x *etc. quibus aequationi* $\mathrm{W} = 0$ *satisfiat, existente* W *functione quacunque illarum litterarum* z, y, x *etc., atque* P, Q, R *etc. ejusmodi fuerint quantitates, ut* $\mathrm{P} \pm \mathrm{W}$, $\mathrm{Q} \pm \mathrm{W}$, $\mathrm{R} \pm \mathrm{W}$ *etc. fiant quadrata: tum iisdem valoribus pro* z, y, x, *etc. assumtis, fient quoque quantitates* P, Q, R *etc. quadrata.*

Ratio hujus lemmatis est manifesta, quia pro litteris z, y, x etc. tales valores assumi ponuntur, ut fiat $W = 0$, ideoque si $P \pm W$, $Q \pm W$, $R \pm W$ sint quadrata, etiam quantitates, P, Q, R, ipsae quadrata sint necesse est.

2. **Coroll. 1.** Formulae quoque P, Q, R etc. reddentur quadrata, si fuerint $P + \alpha W$, $Q + \beta W$, $R + \gamma W$ etc. quadrata, vel etiam generalius, si istae expressiones:

$$P + \alpha W + \zeta W^2, \quad Q + \beta W + \eta W^2, \quad R + \gamma W + \vartheta W^2$$

fuerint quadrata.

3. **Coroll. 2.** Vicissim ergo etiam si litteris z, y, x etc. tales assignati fuerint valores, ut fiat $W = 0$, tum etiam omnes hujus generis formulae $PP + \alpha W$, $QQ + \beta W$, $RR + \gamma W$ etc. fient quadrata.

4. **Coroll. 3.** Quodsi ergo aequationi $W = 0$ infinitis diversis modis satisfieri queat, tum iisdem modis omnes hujus generis formulae $PP + \alpha W$, $QQ + \beta W$, $RR + \gamma W$ etc. quadrata efficientur.

5. **Coroll. 4.** Cum igitur numerus hujusmodi formularum in infinitum augeri possit, manifestum est, quomodo etiam infinitae conditiones praescribi possint, quibus omnibus satisfiat, simul atque unicae conditioni, scilicet aequationi $W = 0$, fuerit satisfactum.

6. **Coroll. 5.** Simili modo hoc lemma ad cubos aliasve potestates altiores quascunque extenditur. Si enim factum fuerit $W = 0$, tum quoque omnes hujusmodi formulae $P^3 + \alpha W$ fient cubi, et hae $P^4 + \alpha W$ biquadrata et ita porro, quaecunque etiam quantitates pro P accipiantur.

7. **Scholion 1.** Ratio quidem hujus lemmatis tam est obvia, ut id nihil in recessu habere videatur: si enim P, Q, R etc. cum W fuerint functiones quaecunque litterarum z, y, x etc. harumque valores quaerantur, quibus sequentes formulae: $PP + \alpha W$, $QQ + \beta W$, $RR + \gamma W$ etc. fiant quadrata, statim utique in oculos incurrit, his omnibus conditionibus satisfieri, dum modo haec una $W = 0$ adimpleatur: verum plerumque ratio talis compositionis in formulis propositis tam est occulta, ut difficillimum sit eam quantitatem W assignare, qua deleta partes residuae formularum sponte fiant quadrata. Quin etiam non adeo foret difficile hanc compositionem ita abscondere, ut ejus investigatio jam per se arduum problema constitueret. Vicissim autem data aequatione $W = 0$, operam haud inutiliter collocari arbitror, si formulae simpliciores investigentur, quae tum in quadrata abibunt; hoc enim modo plurima insignia et concinna reperientur problemata, quorum solutio erit in promtu, cujusmodi est id, cujus supra mentio est facta. Hunc in finem aequationem $W = 0$ talem assumi conveniet, ut litterae z, y etc. in eam aequaliter ingrediantur, atque inter se permutari patiantur; tum enim si PP ejusmodi fuerit quadratum, ut sit $PP + \alpha W$ quadratum, permutandis litteris z, y, x etc. in PP, unde prodeant QQ, RR etc. etiam $QQ + \alpha W$, et $RR + \alpha W$ fient quadrata.

8. **Scholion 2.** Duplex ergo hinc nascitur tractationis nostrae partitio, primam scilicet constituet litterarum z, y, x etc., circa quas quaestio versatur, numerus, prouti duo, vel tres, vel plures quaeruntur numeri, qui datis conditionibus sint praediti. Alteram partitionem suppeditabit dimensionum numerus, ad quem litterae z, y, x etc. in aequatione $W = 0$ assurgunt; quae aequatio cum ita debeat esse comparata, ut resolutionem admittat, nullius quantitatum altior potestas quam secunda occurrere debet, quia alioquin resolutio in numeris rationalibus absolvi non posset. Quare generalis forma aequationis $W = 0$, quam hic tractabimus erit:

$$0 = \alpha + \beta(z + y + x + \text{etc.}) + \gamma(zy + zx + yx + \text{etc.}) + \delta(zz + yy + xx + \text{etc.})$$
$$+ \varepsilon(zzy + zyy + zzx + zxx + \text{etc.}) + \zeta(zyx + \text{etc.}) + \eta(zzyy + zzxx + yyxx + \text{etc.})$$
$$+ \vartheta(zzyx + zyyx + \text{etc.}) \quad \text{etc.}$$

quandoquidem numeri z, y, x etc. in ea debent esse permutabiles. Secundum hanc duplicem ergo partitionem sequentia problemata contemplemur, ab iis inchoaturi, in quibus duo numeri z et y quaerendi proponuntur.

9. **Problema 1.** Proposita hac aequatione resolvenda: $\alpha = \beta(z + y)$, invenire formulas simpliciores, quae per ejus resolutionem redduntur quadrata.

Solutio. Cum huic aequationi $\alpha = \beta(z + y)$ fuerit satisfactum, manifestum est, simul hanc formam generalem $PP + M(-\alpha + \beta(y + z))$ fieri quadratum, quaecunque quantitates pro P et M accipiantur. Quia β evanescere nequit, ponamus $\beta = 1$, ut inter y et z haec subsistat relatio $y + z = a$, sitque $PP + M(y + z - a) =$ quadrato, unde sequentes casus notatu dignos evolvamus:

I. Sit $M = 2$, erit $PP + 2y + 2z - 2a =$ quadrato. Capiatur $P = y - 1$, erit

1) $yy + 2z + 1 - 2a = \square$ et permutatione facta

2) $zz + 2y + 1 - 2a = \square$.

Capiatur $P = y + z - 1$, erit

3) $(y + z)^2 + 1 - 2a = \square$.

Capiatur $P = y - z + 1$, erit

4) $(y - z)^2 + 4y + 1 - 2a = \square$.

5) $(y - z)^2 + 4z + 1 - 2a = \square$.

II. Sit $M = -2$ unde $PP - 2y - 2z + 2a =$ quadrato. Capiatur $P = y + 1$, seu $P = z + 1$, erit

6) $yy - 2z + 1 + 2a = \square$.

7) $zz - 2y + 1 + 2a = \square$.

Capiatur $P = y + z + 1$, erit

8) $(y + z)^2 + 1 + 2a = \square$.

Capiatur $P = y - z + 1$, erit

9) $(y - z)^2 - 4z + 1 + 2a = \square$.

10) $(y - z)^2 - 4y + 1 + 2a = \square$.

III. Sit $M = 2n$, unde $PP + 2ny + 2nz - 2na =$ quadrato, atque non solum formulae praecedentes, sed infinitae aliae, orientur.

Capiatur $P = y - n$ et $P = z - n$, erit

11) $yy + 2nz + nn - 2na = \square$.

12) $zz + 2ny + nn - 2na = \square$.

Capiatur $P = y - 2n$ et $P = z - 2n$, erit

13) $yy - 2ny + 2nz + 4nn - 2na = \square$.

14) $zz - 2nz + 2ny + 4nn - 2na = \square$.

Capiatur $P = y + z - n$, erit

15) $(y + z)^2 + nn - 2na = \square$.

Capiatur $P = y + z - 2n$, erit

16) $(y + z)^2 - 2n(y + z) + 4nn - 2na = \square$.

Capiatur $P = y - z - n$, erit

17) $(y - z)^2 + 4nz + nn - 2na = \square$.

18) $(y - z)^2 + 4ny + nn - 2na = \square$.

IV. Sit $M = -y$, unde $PP - yy - yz + ay =$ quadrato.

Capiatur $P = y$, erit

19) $-yz + ay = \square$.

20) $-yz + az = \square$.

Capiatur $P = y - \frac{1}{2}a$, erit

21) $-yz + \frac{1}{4}aa = \square$.

Capiatur $P = y + z$, erit

22) $zz + yz + ay = \square$.

23) $yy + yz + az = \square$.

Capiatur $P = y + z - \frac{1}{4}a$, erit

24) $zz + yz + \frac{1}{2}ay - \frac{1}{2}az + \frac{1}{16}aa = \square$.

25) $yy + yz + \frac{1}{2}az - \frac{1}{2}ay + \frac{1}{16}aa = \square$.

V. Sit $M = -z - y$, unde $PP - (y + z)^2 + a(y + z) =$ quadrato.

Capiatur $P = y + z$, erit

26) $ay + az = \square$.

Capiatur $P = y + z - a$, erit

27) $aa - ay - az = \square$.

Capiatur $P = y - z$, erit

28) $-4yz + a(y + z) = \square$.

Capiatur $P = y - z - \frac{1}{2}a$, erit

29) $-4yz + 2az + \frac{1}{4}aa = \square$.

30) $-4yz + 2ay + \frac{1}{4}aa = \square$.

Capiatur $P = y - \frac{1}{2}a$, erit

31) $-zz - 2yz + az + \frac{1}{4}aa = \square$.

32) $-yy - 2yz + ay + \frac{1}{4}aa = \square$.

VI. Sit $M = y + z + a$, unde $PP + (y + z)^2 - aa =$ quadrato.

Capiatur $P = yz - 1$, erit

$$33)\quad yyzz + yy + zz + 1 - aa = \square.$$

VII. Sit $M = n(y + z + a)$; unde $PP + n(y + z)^2 - naa =$ quadrato.

Capiatur $P = yz - n$, erit

$$34)\quad yyzz + nyy + nzz + nn - naa = \square.$$

VIII. Sit $M = (y + z + a)(y - z + a)(z - y + a)$, unde fit

$$PP - y^4 - z^4 - a^4 + 2yyzz + 2aayy + 2aazz = \text{quadrato}.$$

Capiatur $P = yy - zz$, erit

$$35)\quad 2yy + 2zz - aa = \square.$$

Capiatur $P = yy + zz + aa$, erit

$$36)\quad yyzz + aayy + aazz = \square.$$

IX. Sit $M = 3(y + z + a)(y - z + a)(z - y + a)$, unde fit

$$PP - 3y^4 - 3z^4 - 3a^4 + 6yyzz + 6aayy + 6aazz = \text{quadrato}.$$

Capiatur $P = 2yy + 2zz + 2aa$, erit

$$37)\quad y^4 + z^4 + 14yyzz + 14aayy + 14aazz + a^4 = \square.$$

Capiatur $P = 2yy + 2zz - 2aa$, erit

$$38)\quad y^4 + z^4 + a^4 + 14yyzz - 2aayy - 2aazz = \square.$$

$$39)\quad y^4 + z^4 + a^4 - 2yyzz + 14aayy - 2aazz = \square.$$

$$40)\quad y^4 + z^4 + a^4 - 2yyzz - 2aayy + 14aazz = \square.$$

X. Sit generalius $M = (nn - 1)(y + z + a)(y - z + a)(z - y + a)$, unde fit

$$PP - (nn - 1)(y^4 + z^4 + a^4 - 2yyzz - 2aayy - 2aazz) = \text{quadrato}.$$

Capiatur $P = n(yy + zz + aa)$, erit

$$41)\quad y^4 + z^4 + a^4 + 2(2nn - 1)(yyzz + aayy + aazz) = \square.$$

Capiatur $P = n(yy + zz - aa)$, erit

$$42)\quad y^4 + z^4 + a^4 + 2(2nn - 1)yyzz - 2aayy - 2aazz = \square.$$

$$43)\quad y^4 + z^4 + a^4 - 2yyzz + 2(2nn - 1)aayy - 2aazz = \square.$$

$$44)\quad y^4 + z^4 + a^4 - 2yyzz - 2aayy + 2(2nn - 1)aazz = \square.$$

10. **Coroll. 1.** Ex his satis intelligitur infinitas exhiberi posse formulas, quae omnes per eandem relationem aequatione $y + z = a$ contentam in numeros quadratos abeant. Quotcunque ergo formulae proponantur ad quadrata reducendae, dummodo illae in his erutis contineantur, omnibus simul satisfiet ponendo $y + z = a$.

11. **Coroll. 2.** Ita si a sit $= 1$: sequentibus formulis omnibus:
$yy + 4z = \square$, $yy - y + z = \square$, $y + z = \square$, $y - yz = \square$, $zz + 4y = \square$, $zz - z + y = \square$, $(y + z)^2 - 1 = \square$, $z - yz = \square$, $yyzz + yy + zz = \square$, $2yy + 2zz - 1 = \square$, satisfit ponendo $y + z = 1$, seu $y = 1 - z$.

12. **Coroll. 3.** Imprimis hic notanda est forma $yyzz + yy + zz$, quae in quadratum transit, si capiatur $y = 1 - z$, vel magis generaliter $y = \pm 1 \pm z$. Solutio haec apud Diophantum

frequentissime occurrit, cujus fundamentum in porismate quodam constituit, pluraque affert problemata, quae ejus beneficio resolvuntur.

13. **Coroll. 4.** Simili modo haec forma latius patens $yyzz + aayy + aazz$ redditur quadratum, ponendo $y = \pm a \pm z$. Atque haec eadem positio facit etiam hanc formam

$$yyzz + nyy + nzz + nn - naa$$

quadratum, quicunque numerus pro n assumatur. Unde si $a = 1$, haec forma

$$yyzz + nyy + nzz + nn - n$$

sive haec

$$(yy + n)(zz + n) - n,$$

fit quadratum, ponendo $z = y \pm 1$. Quod etiam est insigne porisma Diophanti.

14. **Scholion.** Omni attentione utique dignum est, quod tam levi opera pluribus conditionibus simul satisfieri possit, cum quaelibet conditio peculiarem operationem exigere videatur. Quin etiam hic ejusmodi formulae occurrunt, quae si solae proponerentur, per methodos consuetas non nisi difficulter resolvi possent, cujusmodi est haec:

$$y^4 + z^4 + a^4 + 14yyzz + 14aayy + 14aazz = \text{quadrato},$$

cujus solutio si more consueto tentetur, non exiguis difficultatibus implicata deprehenditur: ex quo, si praeterea aliae conditiones praescribantur, quibus simul satisfieri oporteat, quaestio non immerito plus quam determinata, ac vires analyseos transcendens videri debet. Continetur ergo in evolutione hujus problematis jam porisma amplissimum, quod in analysi Diophantea summum habet usum, quod cum natum sit ex positione simplicissima $z + y = a$, ita formulae magis compositae nos ad profundiora ac magis recondita porismata manuducent.

15. **Problema 2.** Proposita hac aequatione resolvenda: $yz - a(y + z) + b = 0$, invenire formulas notabiliores, quae per ejus resolutionem redduntur quadrata.

Solutio. Sumta relatione inter numeros y et z ex hac aequatione $yz - a(y + z) + b = 0$, haec forma generalis $PP + M(yz - a(y + z) + b)$ evadet quadratum; cujus ergo species notabiliores evolvamus.

I. Sit $M = 2$, ut habeatur $PP + 2yz - 2a(y + z) + 2b = \text{quadrato}$.

Capiatur $P = y - z$, eritque

$$1)\quad yy + zz - 2a(y + z) + 2b = \square.$$

Capiatur $P = y - z + a$, erit

$$2)\quad yy + zz - 4az + 2b + aa = \square.$$

$$3)\quad yy + zz - 4ay + 2b + aa = \square.$$

II. Sit $M = -2$, ut habeatur $PP - 2yz + 2a(y + z) - 2b = \text{quadrato}$.

Capiatur $P = y + z$, erit

$$4)\quad yy + zz + 2a(y + z) - 2b = \square.$$

Capiatur $P = y + z - a$, erit

$$5)\quad yy + zz + aa - 2b = \square.$$

III. Sit $M = 2n$, ut habeatur $PP + 2nyz - 2na(y + z) + 2nb = \text{quadrato}$.

Capiatur $P = yz - n$, erit

$$6)\quad yyzz - 2na(y + z) + 2nb + nn = \square.$$

Capiatur $P = y + z + na$, erit

$$7) \quad yy + zz + 2(n+1)yz + nnaa + 2nb = \square.$$

IV. Sit $M = yz + a(y+z) - h$, ut habeatur

$$PP + yyzz - aa(y+z)^2 + (b-h)y + a(b+h)(y+z) - bh = \text{quadrato}.$$

Capiatur $P = m(y+z) + n$, ut sit

$$yyzz + (mm - aa)(y+z)^2 + (b-h)yz + 2mn(y+z) + nn$$
$$+ a(b+h)(y+z) - bh = \text{quadrato}.$$

Fiat $$mn = -\tfrac{1}{2}a(b+h) \text{ et } 2(mm-aa) + b - h = 0, \text{ sive}$$

$$n = \frac{a}{m}(aa - mm - b) \quad \text{et} \quad h = b + 2(mm - aa), \quad \text{erit}$$

$$8) \quad yyzz + (mm-aa)(yy+zz) + \frac{aa-mm}{mm}(bb + (aa-2b)(aa-mm)) = \square.$$

16. **Coroll. 1.** Hinc in aequatione canonica $yz - a(y+z) + b = 0$ litterae a et b ita determinari possunt, ut haec forma $yyzz + cc(yy+zz)$ fiat quadratum.

Capiatur enim $mm = aa + cc$, et fiat $bb + 2bcc - aacc = 0$, seu $b = -cc \pm c\sqrt{(aa+cc)}$. Quare pro a ejusmodi sumatur numerus, ut $aa + cc$ fiat quadratum, tumque erit

$$yz - a(y+z) - cc \pm c\sqrt{(aa+cc)} = 0,$$

sive $$(y-a)(z-a) = aa + cc \pm c\sqrt{(aa+cc)}.$$

At vero hinc conficietur:

$$\sqrt{(yyzz + ccyy + cczz)} = (y+z)\sqrt{(aa+cc)} - ac.$$

17. **Coroll. 2.** Ad formam ergo $yyzz + ccyy + cczz$ quadratum reddendam sumatur primum numerus a, ut $\sqrt{(aa+cc)}$ fiat rationale, eritque tum

$$z = \frac{ay + cc \pm c\sqrt{(aa+cc)}}{y-a}.$$

Haec autem solutio simul praecedentem ejusdem formae in se complectitur, casu, quo a capitur infinitum, tum enim oritur $z = -y \pm c$, omnino ut ante, ideoque haec solutio latius patet quam illa.

18. **Coroll. 3.** Si in forma (8) nulla limitatio fiat, ita ut aequatio proposita

$$yz - a(y+z) + b = 0$$

generatim valeat, ea etiam hoc modo referri potest

$$(yy + mm - aa)(zz + mm - aa) - \frac{(mm-aa)}{mm}(mm - aa + b)^2 = \text{quadrato}.$$

Quare posito $mm - aa = p$ et $b + p = m = \sqrt{(aa+p)}$, haec aequatio:

$$(yy+p)(zz+p) = VV + p$$

resolvetur hac determinatione $yz - a(y+z) - p + \sqrt{(aa+p)} = 0$, dummodo pro a talis accipiatur numerus, quo $aa + p$ fiat quadratum.

19. **Coroll. 4.** Si statuatur $\frac{b+p}{m} = q$, seu $b = -p + q\sqrt{(aa+p)}$, ut sit

$$yz - a(y+z) - p + q\sqrt{(aa+p)} = 0$$

hac determinatione, si modo $aa + p$ fuerit quadratum, satisfiet huic conditioni

$$(yy+p)(zz+p) = VV + pqq,$$

erit autem $V = (y+z)\sqrt{(aa+p)} - aq$.

20. **Coroll. 5.** Hinc si dato numero p quaerantur numeri y et z, ut fiat

$$(yy+p)(zz+p) = \text{quadrato},$$

posito $q=0$, huic conditioni satisfiet statuendo $yz - a(y+z) - p = 0$, existente $aa+p$ numero quadrato. Seu sumatur $(y-a)(z-a) = aa+p$, unde si $aa+p$ in factores resolvatur, commode ambo numeri y et z definiuntur.

21. **Coroll. 6.** Si sit $a=0$, forma (8) fiet: $yyzz + mm(yy+zz) - bb - 2mmb = \square$, quae conditio ergo adimplebitur hac aequatione $yz + b = 0$. Facto ergo $b = -2mm$, ista formula $yyzz + mmyy + mmzz$ reddetur quadratum, sumendo $yz = 2mm$, quod quidem per se est manifestum.

22. **Problema 3.** Proposita aequatione resolvenda $yy + zz - 2nyz - a = 0$, invenire formulas notabiliores, quae per eam redduntur quadrata.

Solutio. Hinc ergo ista forma generalis erit quadratum

$$PP + M(yy+zz-2nyz-a) = \text{quadrato}.$$

I. Sit $M = -1$ et $P = y \pm z$, erit

1) $2(n+1)yz + a = \square$.

2) $2(n-1)yz + a = \square$.

II. Sit $M = m$ et $P = yz + mn$, erit

3) $yyzz + myy + mzz - ma + mmnn = \square$.

III. Sit $M = 2nyz$ et $P = 2nyz$, erit

4) $2nyz(yy+zz) - 2nayz = \square$.

IV. Sit $M = -zz$ et $P = zz + nyz + \frac{1}{2}a$, erit

5) $(nn-1)yyzz + nayz + \frac{1}{4}aa = \square$.

23. **Coroll. 1.** Si ponamus $a = mnn$, pervenimus ad hanc formam $yyzz + myy + mzz$, quae ergo redditur quadratum per hanc aequationem: $yy + zz - 2nyz - mnn = 0$, unde fit $z = ny \pm \sqrt{((nn-1)yy + mnn)}$. Quare pro y talis numerus assumi debet, ut $(nn-1)yy + mnn$ fiat quadratum.

24. **Coroll. 2.** Quoniam hic numerus n arbitrio nostro relinquitur, sumatur talis, ut $nn-1$ prodeat quadratum, sic enim commodissime forma $(nn-1)yy + mnn$ ad quadratum reducetur: capiatur scilicet $n = \frac{kk+1}{2k}$.

25. **Scholion.** Hisce formulis, quae duas indeterminatas involvunt, fusius non immoror, quoniam ex allatis perspicuum est, quomodo hujusmodi formularum investigationem in infinitum extendere liceat. Pergo igitur ad tres indeterminatas, ubi plurima egregia porismata occurrunt, quorum praecipua hic explicabo.

26. **Problema 4.** Proposita hac aequatione resolvenda: $a = x + y + z$, definire formulas notabiliores, quae per ejus resolutionem quadrata redduntur.

Solutio. Quadratum ergo generatim erit haec forma: $PP + M(x + y + z - a)$.

Sit $M = 2n$, ut fiat $PP + 2n(x + y + z) - 2na = \square$.

Capiatur $P = x - n$, erit

1) $xx + 2n(y + z) + nn - 2na = \square$.

2) $yy + 2n(x + z) + nn - 2na = \square$.

3) $zz + 2n(x + y) + nn - 2na = \square$.

Capiatur $P = x + y - n$, erit

4) $(x + y)^2 + 2nz + nn - 2na = \square$.

5) $(x + z)^2 + 2ny + nn - 2na = \square$.

6) $(y + z)^2 + 2nx + nn - 2na = \square$.

Sit $M = 2nxy$ et $P = xy - nx - ny$, erit

7) $xxyy + 2nxyz + nnxx + nnyy + 2n(n - a)xy = \square$.

8) $xxzz + 2nxyz + nnxx + nnzz + 2n(n - a)xz = \square$.

9) $yyzz + 2nxyz + nnyy + nnzz + 2n(n - a)yz = \square$.

Sit $M = -(a + x + y + z)$ et $P = x + y - z$, erit

10) $aa - 4xz - 4yz = \square$.

11) $aa - 4xy - 4yz = \square$.

12) $aa - 4xy - 4xz = \square$.

Sit $M = -n(a + x + y + z)$ et $P = xy + xz + yz + n$, erit

13) $(xy + xz + yz)^2 - n(xx + yy + zz) + nn + naa = \square$.

27. **Coroll. 1.** Sit $n = 2a$ et $a = \frac{1}{4}$, atque his conditionibus:

$$xx + y + z = \square \qquad (x + y)^2 + z = \square$$
$$yy + x + z = \square \qquad (x + z)^2 + y = \square$$
$$zz + x + y = \square \qquad (y + z)^2 + x = \square$$

satisfiet ponendo $x + y + z = \frac{1}{4}$.

28. **Coroll. 2.** Sit $n = 1 = a$, atque his conditionibus:

$$xxyy + 2xyz + xx + yy = \square$$
$$xxzz + 2xyz + xx + zz = \square$$
$$yyzz + 2xyz + yy + zz = \square$$

satisfiet ponendo $x + y + z = 1$.

29. **Coroll. 3.** Sit $a = 2$, atque his conditionibus

$$1 - xz - yz = \square \qquad 1 - xy - yz = \square \qquad 1 - xy - xz = \square$$

satisfiet ponendo $x + y + z = 2$.

30. **Problema 5.** Proposita hac aequatione resolvenda

$$xy + xz + yz = a(n + y + z) + b$$

definire formulas notabiliores, quae per ejus resolutionem redduntur quadrata.

Solutio. Erit ergo in genere haec formula:

$$PP + M((xy + xz + yz) - a(x + y + z) - b) = \text{quadrato}.$$

Sit $M = 2$, ut habeatur:

$$PP + 2(xy + xz + yz) - 2a(x + y + z) - 2b = \text{quadrato}.$$

Capiatur $P = x + y + z + a$, erit

1) $xx + yy + zz + 4(xy + xz + yz) + aa - 2b = \Box$.

Capiatur $P = x + y - z + a$, erit

2) $xx + yy + zz + 4xy - 4az + aa - 2b = \Box$.

3) $xx + yy + zz + 4xz - 4ay + aa - 2b = \Box$.

4) $xx + yy + zz + 4yz - 4ax + aa - 2b = \Box$.

Capiatur $P = x - y$, erit

5) $xx + yy + 2(x + y)z - 2a(x + y + z) - 2b = \Box$.

6) $xx + zz + 2(x + z)y - 2a(x + y + z) - 2b = \Box$.

7) $yy + zz + 2(y + z)x - 2a(x + y + z) - 2b = \Box$.

Sit $M = -2$ et $P = x + y + z - a$, erit

8) $xx + yy + zz + aa + 2b = \Box$.

31. **Problema 6.** Proposita hac aequatione

$$xx + yy + zz = 2xy + 2xz + 2yz + a$$

definire formulas simpliciores, quae per ejus resolutionem quadrata redduntur.

Solutio. In genere ergo haec formula erit:

$$PP + M(xx + yy + zz - 2xy - 2xz - 2yz - a) = \text{quadrato}.$$

Sit $M = -1$, ac ponatur $P = x + y + z$, erit

1) $4xy + 4xz + 4yz + a = \Box$.

Sit $M = -1$ et $P = x + y - z$, erit

2) $4xy + a = \Box$.

3) $4xz + a = \Box$.

4) $4yz + a = \Box$.

Sit $M = -1$ et $P = x - y$, erit

5) $a + 2(x + y)z - zz = \Box$.

6) $a + 2(x + z)y - yy = \Box$.

7) $a + 2(y + z)x - xx = \Box$.

32. **Coroll. 1.** Posito $a = 4n$, ut sit $xx + yy + zz = 2xy + 2xz + 2yz + 4n$, fient simul sequentes formulae quadrata:

$$xy + n = \Box$$
$$xz + n = \Box$$
$$yz + n = \Box$$
$$\text{et} \quad xy + xz + yz + n = \Box.$$

Unde haec elegans quaestio Diophantea resolvitur:

Dato numero quocunque n, *invenire tres numeros, ut producta ex binis singula, illo numero aucta, fiant quadrata: quibus conditionibus adjungi potest haec, ut summa productorum ex binis eodem numero aucta quoque fiat quadratum.*

33. **Coroll. 2.** Cum enim ex aequatione sit: $z = x + y \pm 2\sqrt{(xy + n)}$, sumantur pro x et y tales numeri, quibus $xy + n$ reddatur quadratum, puta $xy + n = uu$; indeque elicietur duplex valor pro numero z, scilicet $z = x + y \pm 2u$, quorum uterque cum x et y omnibus conditionibus aeque satisfacit.

34. **Coroll. 3.** Cum autem sit $\sqrt{(xy + n)} = u$, erunt, sumto tertio numero $z = x + y + 2u$, reliquae formulae

$$\sqrt{(xz + n)} = \frac{x + z - y}{2} = x + u,$$

$$\sqrt{(yz + n)} = \frac{y + z - x}{2} = y + u,$$

$$\sqrt{(xy + xz + yz + n)} = \frac{x + y + z}{2} = x + y + u.$$

35. **Problema 7.** Proposita hac aequatione:

$$xx + yyzz = 2xy + 2yz + 2xz + 2a(x + y + z) + b$$

definire formulas notabiliores, quae per ejus resolutionem redduntur quadrata.

Solutio. In genere ergo quadratum erit haec forma:

$$PP + M(xx + yy + zz - 2xy - 2yz - 2xz - 2a(x + y + z) - b).$$

Sit $M = -1$ et capiatur $P = x + y + z + a$, erit

1) $4xy + 4xz + 4yz + 4a(x + y + z) + aa + b = \square$.

Capiatur $P = x + y + z - a$, erit

2) $4xy + 4xz + 4yz + aa + b = \square$.

Capiatur $P = x + y - z + a$, erit

3) $4xy + 4a(x + y) + aa + b = \square$.

4) $4xz + 4a(x + z) + aa + b = \square$.

5) $4yz + 4a(y + z) + aa + b = \square$.

Capiatur $P = x + y - z - a$, erit

6) $4xy + 4az + aa + b = \square$.

7) $4xz + 4ay + aa + b = \square$.

8) $4yz + 4ax + aa + b = \square$.

36. **Coroll. 1.** Ad formulas has facillime solvendas, ponatur tertia

$$4xy + 4a(x + y) + aa + b$$

aequalis quadrato cuipiam uu, et ob

$$4(x + a)(y + a) = uu - b + 3aa, \quad \text{seu} \quad (x + a)(y + a) = \tfrac{1}{4}(uu - b + 3aa),$$

ex factoribus numeri $\frac{1}{4}(uu - b + 3aa)$ commodissime definiuntur numeri duo x et y; tertius autem z colligitur ex formae tertiae radice quadrata $x + y - z + a$, quae ergo est $= u$, unde fit $z = x + y + a \pm u$.

37. **Coroll. 2.** Si sit $b = -aa$, per resolutionem hujus aequationis

$$xx + yy + zz = 2xy + 2yz + 2xz + 2a(x + y + z) - aa$$

sequentes formulae omnes in quadrata abibunt:

$$xy + a(x + y) = \square, \quad xy + az = \square,$$
$$xz + a(x + z) = \square, \quad xz + ay = \square,$$
$$yz + a(y + z) = \square, \quad yz + ax = \square,$$
$$xy + xz + yz = \square,$$
$$xy + xz + yz + a(x + y + z) = \square.$$

Satisfiet autem sumendo: $z = x + y + a \pm 2\sqrt{(xy + a(x + y))} = x + y + a \pm 2u$ posito $(x + a)(y + a) = uu + aa$.

38. **Coroll. 3.** In hoc corollario continetur illud ipsum problema, cujus initio feci mentionem, si quidem ponatur $a = 1$. Atque ex iisdem formulis solvi quoque potest quaestio, in qua ipsi numeri x, y, z quadrati esse debent, cujus solutionem hic subjungam.

39. **Quaestio.** *Invenire tres numeros quadratos, ut ad productum binorum, sive eorundem summa, sive reliquus addatur, quadratum prodeat, atque ut insuper tam summa productorum ex binis ipsa, quam eadem, summa numerorum aucta, fiat quadratum.*

Solutio. Positis ergo xx, yy, zz quadratis, qui quaeruntur, sequentes formulas quadrata reddi oportet:

$$xxyy + xx + yy = \square, \quad xxyy + zz = \square,$$
$$xxzz + xx + zz = \square, \quad xxzz + yy = \square,$$
$$yyzz + yy + zz = \square, \quad yyzz + xx = \square,$$
$$xxyy + xxzz + yyzz = \square,$$
$$xxyy + xxzz + yyzz + xx + yy + zz = \square.$$

His autem omnibus satisfit, dummodo statuatur

$$zz = xx + yy + 1 \pm 2\sqrt{(xxyy + xx + yy)}.$$

Supra autem vidimus, formam $xxyy + xx + yy$ quadratum fieri, si ponatur $y = x + 1$. Sit igitur $y = x + 1$, eritque

$$zz = 2xx + 2x + 2 \pm 2\sqrt{(x^4 + 2x^3 + 3xx + 2x + 1)} \quad \text{seu} \quad zz = 4(xx + x + 1).$$

Tantum ergo superest, ut $xx + x + 1$ reddatur quadratum, quod posita radice $-x + t$ praebet

$$x = \frac{tt - 1}{2t + 1}, \quad \text{et} \quad \sqrt{(xx + x + 1)} = \frac{tt + t + 1}{2t + 1}$$

unde fit

$$z = 2\sqrt{(xx + x + 1)} = \frac{2(tt + t + 1)}{2t + 1}.$$

Quadratorum ergo trium quaesitorum radices sunt:

$$x = \frac{tt - 1}{2t + 1}, \quad y = \frac{tt + 2t}{2t + 1}, \quad z = \frac{2tt + 2t + 2}{2t + 1}.$$

Vel quo facilius pro t fractiones capi queant, statuatur

$$t = \frac{r-q}{2q}, \quad \text{eruntque hae radices}$$

$$x = \frac{3qq + 2qr - rr}{4qr}, \quad y = \frac{rr + 2qr - 3qq}{4qr}, \quad z = \frac{rr + 3qq}{2qr};$$

unde sumto $r = 2$ et $q = 1$, oriuntur hi valores

$$x = \frac{3}{8}, \quad y = \frac{5}{8}, \quad z = \frac{7}{4},$$

quibus solutio supra tradita continetur. Simplicior fortasse solutio est:

$$x = \frac{3}{5}, \quad y = \frac{8}{5} \quad \text{et} \quad z = \frac{14}{5}.$$

40. **Scholion.** His praeceptis observandis facile erit numerum talium formularum pro lubitu multiplicare, easque tam ad quatuor indeterminatas, quam ad formas magis compositas extendere. Quin etiam simili modo plures formae exhiberi poterunt, quae per certam positionem cubi redduntur; sed quoniam in iis non amplius tanta cernitur concinnitas, hanc meditationem finiendam esse censeo, cum id, quod mihi praecipue erat propositum, ut novum analyseos Diophanteae supplementum producerem, abunde explicaverim.



XIX.

Theoremata circa residua ex divisione potestatum relicta.

(N. Comment. VII. 1758 — 59. p. 49.)

1. **Theorema 1.** Si p sit numerus primus, et a primus ad p, nullus terminus hujus progressionis geometricae $1, a, a^2, a^3, a^4, a^5, a^6$, etc. per numerum p divisibilis existit.

Demonstratio patet ex Euclidis libro VII. prop. 26, ubi demonstratur, si sint duo numeri a et b primi ad p, fore quoque productum ab primum ad p; ideoque cum a sit primus ad p, erit posito $b=a$, quadratum a^2 primus ad p; hincque porro a^3 posito $b=a^2$; item a^4 posito $b=a^3$, etc. Sic igitur nulla potestas ipsius a divisibilis erit per numerum primum p.

2. **Coroll. 1.** Si igitur singuli termini progressionis geometricae

$$1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, \text{etc.}$$

per numerum primum p dividantur, divisio nunquam sine residuo succedet, sed ex singulis terminis orientur residua.

3. **Scholion.** Residua haec, quae ex divisione singulorum terminorum progressionis propositae geometricae per numerum primum p emergunt, hic diligentius perpendere constitui. Ac primo quidem singula haec residua, uti ex natura divisionis apparet, minora erunt numero p; nullum autem residuum erit $=0$, quia nullus terminus per p est divisibilis. Quodsi forte prodeant residua ipso numero p majora, ex arithmetica constat, quemadmodum ea ad minora reduci oporteat. Sic residuum $p+r$ aequivalet residuo r, et in genere residuum $np+r$ redit ad residuum r; ac si r sit majus quam p, hoc residuum revocatur ad $r-p$, vel $r-2p$, vel $r-3p$, etc. donec ad numerum ipso p minorem perveniatur. Itaque omnia haec residua $r \pm np$ pro eodem residuo r reputantur. Proprie autem loquendo omnia residua sunt numeri positivi ipso divisore p minores. Verum tamen etiam saepenumero convenit et residua negativa contemplari: veluti si r sit residuum ex divisione cujuspiam numeri per p relictum, ita ut sit $r<p$, residuum quoque erit $r-p$, numerus scilicet negativus; ita ut residuum positivum r aequivaleat residuo negativo $r-p$. Hoc modo residua ita exhiberi poterunt, ut nunquam semissem divisoris p excedant: nam si residuum affirmativum r majus fuerit quam $\frac{1}{2}p$, ejus loco capiatur residuum negativum $r-p$, quod minus erit, quam semissis ipsius p.

4. **Coroll. 2.** Quoniam omnia residua sunt numeri integri, iique minores quam p: sequitur plura diversa residua oriri non posse quam $p-1$. Quare cum series geometrica $1, a, a^2, a^3, a^4, a^5$, etc., ex terminis numero infinitis constet, necesse est, ut plures termini eadem exhibeant residua.

5. **Coroll. 3.** Sint a^μ et a^ν duo ejusmodi termini, qui idem praebeant residuum r; ita ut sit $a^\mu = mp + r$ et $a^\nu = np + r$, erit $a^\mu - a^\nu = (m - n)p$, ideoque differentia horum terminorum $a^\mu - a^\nu$ per p erit divisibilis. Innumeris ergo modis differentia inter binos terminos progressionis geometricae propositae per numerum p erit divisibilis.

6. **Coroll. 4.** Si potestas a^μ det residuum r, potestas vero a^ν residuum s, fueritque $r + s = p$, quo casu dicimus residuorum r et s alterum alterius esse complementum, hoc casu summa potestatum $a^\mu + a^\nu$ per numerum p erit divisibilis. Cum enim sit $a^\mu = mp + r$ et $a^\nu = np + s$, erit $a^\mu + a^\nu = (m + n)p + r + s = (m + n + 1)p$, ideoque factorem habet p.

7. **Theorema 2.** Si potestas a^μ per p divisa praebeat residuum r, et potestas a^ν residuum s, potestas $a^{\mu+\nu}$ residuum praebebit rs.

Demonstratio. Sit enim $a^\mu = mp + r$ et $a^\nu = np + s$, erit $a^{\mu+\nu} = mnpp + mps + npr + rs$; ideoque si $a^{\mu+\nu}$ per p dividatur, residuum erit rs; quod si majus fuerit quam p, subtrahendo p, quoties fieri potest, id ad residuum ipso divisore p minore reducetur. Q. E. D.

8. **Coroll. 1.** Cum ipsius radicis a per p divisae residuum exponi queat per a, (si enim sit $a < p$, erit a residuum proprie sic dictum, sin autem $a > p$, nihilominus residuum per a exprimere licet, quia simul $a - p$, vel $a - np$ subintelligitur), si potestatis a^μ per p divisae residuum sit r, potestatis $a^{\mu+1}$ residuum erit ar, simili modo potestatis $a^{\mu+2}$ residuum erit $a^2 r$

" $a^{\mu+3}$ " " $a^3 r$, etc.

9. **Coroll. 2.** Hinc etiam sequitur, si potestatis a^μ per p divisae residuum sit $= r$, fore potestatis $a^{2\mu}$ residuum $= rr$, potestatis $a^{3\mu}$ residuum $= r^3$, etc. Ita si potestatis a^μ residuum sit $= 1$, erit omnium harum potestatum $a^{2\mu}$, $a^{3\mu}$, $a^{4\mu}$, $a^{5\mu}$, etc. idem quoque residuum 1.

10. **Coroll. 3.** Quodsi potestatis a^μ per p divisae residuum sit $= p - 1$, quod, ut vidimus, per -1 exponi potest: tum potestatis $a^{2\mu}$ residuum erit $= +1$, potestatis $a^{3\mu}$ residuum $= -1$, at potestatis $a^{4\mu}$ iterum $= +1$. Atque in genere potestatis $a^{n\mu}$ residuum erit, vel $+1$, si n sit numerus par, vel -1, si n sit numerus impar.

11. **Scholion.** Hinc colligitur modus, satis expedite residua inveniendi, quae ex divisione cujuscunque potestatis per numerum quemcunque relinquuntur. Veluti si residuum investigare velimus, quod ex divisione hujus potestatis 7^{160} per numerum 641 oritur:

potestates	residua
7^1	7
7^2	49
7^3	343
7^4	478
7^8	288
7^{16}	255
7^{32}	284
7^{64}	-110
7^{128}	-79
7^{160}	-1

nempe cum potestas prima 7 relinquat 7, potestates vero 7^2, 7^3, 7^4 relinquant 49, 343 et 478, seu -163; hujus quadratum 7^8 relinquet 163^2, seu 288, et quadratum hujus 7^{16} relinquet 288^2, seu 255. Simili modo potestas 7^{32} relinquet 255^2, seu 284, et potestatis 7^{64} residuum erit -110, et ex 7^{128} oritur 110^2, seu -79, quod residuum per 284 multiplicatum, dabit residuum potestatis $7^{128+32} = 7^{160}$, quod erit 640, seu -1.

Novimus ergo, si potestas 7^{160} per 641 dividatur, residuum fore 640, seu -1, unde concludimus potestatis 7^{320} residuum fore $+1$. Ergo in genere potestatis 7^{160n} per 641 divisae residuum erit, vel $+1$, si n sit numerus par, vel -1, si n sit numerus impar.

12. **Theorema 3.** Si numerus a sit primus ad p, formeturque haec progressio geometrica $1, a, a^2, a^3, a^4, a^5, a^6, a^7$, etc. innumeri in ea occurrent termini, qui per p divisi relinquunt pro residuo 1, et exponentes horum terminorum progressionem arithmeticam constituent.

Demonstratio. Quia numerus terminorum est infinitus, plura autem diversa residua oriri nequeunt, quam $p-1$, necesse est ut plures, immo infiniti, termini idem producant residuum r. Sint a^μ et a^ν duo hujusmodi termini, idem residuum r relinquentes, eritque $a^\mu - a^\nu$ per p divisibile. At $a^\mu - a^\nu = a^\nu(a^{\mu-\nu}-1)$, et cum hoc productum sit divisibile per p, alter autem factor a^ν ad p sit primus, necesse est, alter factor $a^{\mu-\nu}-1$ per p sit divisibilis; unde potestas $a^{\mu-\nu}$ per p divisa residuum habebit $=1$. Sit $\mu-\nu=\lambda$, ut potestatis a^λ residuum sit $=1$, eritque omnium quoque harum potestatum $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$, $a^{5\lambda}$ etc. idem residuum $=1$. Itaque unitas erit residuum omnium harum potestatum $1, a^\lambda, a^{2\lambda}, a^{3\lambda}, a^{4\lambda}, a^{5\lambda}, a^{6\lambda}$, etc., quarum exponentes in progressione arithmetica progrediuntur.

13. **Coroll. 1.** Inventa ergo unica potestate a^λ, quae per p divisa residuum praebet $=1$, infinitae inde aliae potestates exhiberi possunt, quae per p divisae quoque unitatem relinquant. Ac infima quidem hujus generis potestas est $a^0=1$.

14. **Coroll. 2.** Etiamsi autem praeter unitatem nulla constet potestas ipsius a, quae per p divisa unitatem pro residuo relinquat, tamen novimus infinitas hujusmodi revera dari potestates.

15. **Coroll. 3.** Ex demonstratione porro patet, dari adeo potestatem a^λ, residuum $=1$ praebentem, cujus exponens λ sit minor quam p. Si enim progressio geometrica tantum usque ad terminum a^{p-1} continuetur, quia terminorum numerus est $=p$, necesse est, ut saltem duo termini, qui sint a^μ et a^ν idem habeant residuum; unde cum potestas $a^{\mu-\nu}$ habitura sit residuum $=1$, ob $\mu<p$ et $\nu<p$, certe erit $\mu-\nu<p$.

16. **Theorema 4.** Si potestas a^μ per p divisa, residuum relinquat $=r$, et potestatis altioris $a^{\mu+\nu}$ residuum sit $=rs$, erit potestatis a^ν, qua haec illam superat, residuum $=s$.

Demonstratio. Praebeat enim potestas a^ν aliud residuum, puta $=t$, et cum potestatis a^μ residuum sit $=r$, erit potestatis $a^{\mu+\nu}$ residuum $=rt$, quod ipsi rs aequivalere deberet. Foret ergo $rt=rs+np$, siquidem ponamus residua r, t esse ipso divisore p minora. Esset ergo $t=s+\frac{np}{r}$; at cum a et p sint numeri inter se primi, omnia residua, quae ex potestatibus ipsius a per p divisis oriuntur, pariter erunt ad p prima, nisi forte sint $=1$; ideoque ut $\frac{np}{r}$ fiat numerus integer, necesse est, ut $\frac{n}{r}$ sit numerus integer, puta $=m$, foretque $t=s+mp$, ideoque $t=s$. Quare si potestatis a^μ residuum sit $=r$, et potestatis $a^{\mu+\nu}$ residuum $=rs$, hinc sequitur potestatis a^ν residuum fore $=s$.

17. **Coroll. 1.** Si ergo $s = 1$, seu si duae potestates a^{μ} et $a^{\mu+\nu}$ idem habeant residuum r, sequitur, si major per minorem dividatur, quoto a^{ν} respondere residuum $= 1$, quo ipso demonstratio praecedentis theorematis innititur.

18. **Coroll. 2.** Si $r = 1$ et $s = 1$, seu si duae potestates a^{μ} et $a^{\mu+\nu}$ idem habeant residuum $= 1$, tum etiam potestas a^{ν}, cujus exponens est differentia illorum exponentium, pariter residuum $= 1$ habebit.

19. **Scholion.** Demonstratio hujus theorematis etiam hoc modo confici potest. Cum a^{μ} per p divisum relinquat r, erit $a^{\mu} = mp + r$, similique modo $a^{\mu+\nu} = np + rs$; hinc erit

$$a^{\mu+\nu} - a^{\mu} s = np - mps = (n - ms)p;$$

ideoque numerus $a^{\mu+\nu} - a^{\mu} s = a^{\mu}(a^{\nu} - s)$ erit per p divisibilis: at alter factor a^{μ} per p non est divisibilis. Ergo alter $a^{\nu} - s$ erit per p divisibilis, consequenter potestas a^{ν} per p divisa residuum dabit $= s$.

20. **Theorema. 5.** Si post unitatem a^{λ} sit minima potestas, quae per p divisa unitatem relinquit, tum nullae aliae potestates idem residuum $= 1$ relinquent, nisi quae in hac progressione geometrica occurrunt

$$1,\ a^{\lambda},\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda},\ a^{5\lambda},\ \text{etc.}$$

Demonstratio. Ponamus enim, aliam quampiam potestatem a^{μ}, si per p dividatur, residuum quoque dare $= 1$, et cum sit $\mu > \lambda$, neque tamen multiplo cuipiam ipsius λ aequetur, hic exponens μ ita exhiberi potest, ut sit $\mu = n\lambda + \delta$, ubi sit $\delta < \lambda$: neque erit $\delta = 0$. Cum igitur tam potestas $a^{n\lambda}$, quam $a^{\mu} = a^{n\lambda+\delta}$, per p divisa unitatem relinquat, per § 18, haec quoque potestas a^{δ} unitatem pro residuo habebit, foretque ergo a^{λ} non minima potestas hujus indolis contra hypothesin. Quare si a^{λ} sit minima potestas residuum $= 1$ praebens, nullae aliae potestates eadem proprietate erunt praeditae, nisi quarum exponentes sunt multipla ipsius λ.

21. **Coroll. 1.** Si ergo progressionis geometricae $1, a, a^2, a^3, a^4$, etc. jam secundus terminus a per p divisus relinquat 1, quod fit, si $a = np + 1$, tum omnes termini idem praebebunt residuum $= 1$: neque ergo in residuis ulli alii numeri praeter 1 occurrent.

22. **Coroll. 2.** Si residuum tertii termini a^2 sit $= 1$, quod fit, si $a^2 = np + 1$, tum alterni termini $1, a^2, a^4, a^6$, etc., quorum exponentes sunt pares, omnes residuum habebunt idem $= 1$, reliqui vero termini, nisi a^1 quoque residuum habeat $= 1$, omnes alia praebebunt residua.

23. **Coroll. 3.** Fieri ergo potest, ut in residuis multo pauciores numeri occurrant, quam numerus $p - 1$ continet unitates: plures autem, quam $p - 1$, diversi numeri occurrere non possunt.

24. **Theorema 6.** Si potestas a^{2n}, cujus exponens est numerus par, per numerum primum p divisa, residuum $= 1$ relinquit, tum potestas a^{n} per eundem numerum p divisa, dabit residuum $= +1$, vel $= -1$.

Demonstratio. Ponamus enim r esse residuum, quod in divisione potestatis a^{n} per numerum primum p relinquitur, eritque potestatis a^{2n} residuum $= rr$, quod per hypothesin $= 1$. Quare erit $rr = 1 + mp$ et $rr - 1 = mp$; unde cum $rr - 1 = (r + 1)(r - 1)$ sit divisibile per p, alterutrum

factorem $r+1$, vel $r-1$ per p divisibilem esse oportet. Priori casu erit $r+1=up$, et $r=up-1$, hincque $r=-1$. Posteriori casu erit $r-1=up$ et $r=up+1$, hincque $r=+1$. Ergo si potestas a^{2n} residuum praebeat $=+1$, potestas a^n habebit vel residuum $=+1$, vel $=-1$, siquidem p sit numerus primus.

25. **Coroll. 1.** Si igitur a^{2n} fuerit minima potestas, quae per numerum primum p divisa residuum relinquit $=+1$, tum potestas a^n residuum dabit $=-1$. Ergo si minimae potestatis a^λ residuum $=1$ praebentis, exponens λ sit numerus par, tum inter residua terminorum progressionis geometricae $1, a, a^2, a^3, a^4$, etc. etiam occurret numerus -1.

26. **Coroll. 2.** Sin autem minimae potestatis a^λ residuum 1 praebentis, exponens λ sit numerus impar, tum nulla omnino potestas residuum relinquet $=-1$. Si enim quaepiam potestas, uti a^μ, daret residuum $=-1$, tum potestas $a^{2\mu}$ daret residuum $=+1$, foretque idcirco $2\mu=n\lambda$, et quia λ est numerus impar, foret $2\mu=2m\lambda$, ideoque $\mu=m\lambda$. At potestas $a^{m\lambda}$ relinquit residuum $=+1$, neque ergo residuum -1 usquam occurrere potest.

27. **Theorema 7.** Si a^λ fuerit minima potestas ipsius a, quae per numerum p divisa, residuum praebet $=1$, tum omnia residua, quae ex terminis progressionis geometricae $1, a, a^2, a^3 \ldots . a^{\lambda-1}$, usque ad illam potestatem a^λ continuatae, resultant, erunt inter se inaequalia.

Demonstratio. Si enim duae potestates, veluti a^μ et a^ν, quarum exponentes μ et ν sint minores quam λ, idem darent residuum, tum earum differentia $a^\mu - a^\nu$ foret per p divisibilis, ideoque potestas $a^{\mu-\nu}$ per p divisa residuum relinqueret $=+1$, essetque idcirco $\mu-\nu<\lambda$, contra hypothesin, unde patet, omnes potestates, quarum exponentes sint minores, quam λ, diversa praebere residua.

28. **Theorema 8.** Si a^λ fuerit quaedam potestas ipsius a, quae per numerum p divisa residuum producat $=1$, atque progressio geometrica in membra discerpatur, secundum potestates $a^\lambda, a^{2\lambda}, a^{3\lambda}, a^{4\lambda}$, etc. hoc modo:

$$1, a, a^2 \ldots a^{\lambda-1} \mid a^\lambda \ldots a^{2\lambda-1} \mid a^{2\lambda} \ldots a^{3\lambda-1} \mid a^{3\lambda} \ldots a^{4\lambda-1} \mid \text{etc.}$$

ita ut quodvis membrum λ terminos contineat, tum in quolibet membro residua prodibunt eadem, atque eodem ordine recurrent.

Demonstratio. Omnium enim membrorum termini primi $1, a^\lambda, a^{2\lambda}, a^{3\lambda}$, etc. idem praebent residuum $=1$. Termini deinde secundi omnium membrorum $a, a^{\lambda+1}, a^{2\lambda+1}, a^{3\lambda+1}$, etc. idem pariter dabunt residuum; sit enim r residuum ex termino a^1 ortum, quia $a^{\lambda+1}=a^\lambda a^1$, erit residuum ex hoc termino ortum $=1.r=r$; similique modo patet, terminorum $a^{2\lambda+1}, a^{3\lambda+1}$ etc. residua fore $=r$. Ac si in genere sit a^μ terminus quotuscunque primi membri, atque residuum ex eo ortum $=r$, erit quoque termini $a^{n\lambda+\mu}$ residuum $=r$, quia termini $a^{n\lambda}$ residuum est $=1$: hincque omnium membrorum termini analogi $a^{\lambda+\mu}, a^{2\lambda+\mu}, a^{3\lambda+\mu}$ etc. idem habebunt residuum.

29. **Coroll. 1.** Quodsi ergo tantum terminorum in primo membro contentorum residua fuerint cognita, tum omnium quoque terminorum, qui reliqua membra constituunt, residua erunt cognita.

30. **Coroll. 2.** Si enim proponatur terminus a^x, cujus exponens x sit numerus quantumvis magnus, ejus residuum facile reperietur. Iste enim exponens x ad hanc formam $n\lambda + \mu$ reduci potest, ut sit $\mu < \lambda$, atque residuum termini a^x idem erit, quod termini a^μ.

31. **Coroll. 3.** Hic autem numerus μ minor quam λ invenitur, si numerus x per λ dividatur, tum enim residuum, quod in hac divisione remanet, erit hic ipse numerus μ, qui quaeritur.

32. **Coroll. 4.** Semper autem datur potestas a^λ, quae per p divisa unitatem relinquit, cujus exponens λ minor sit quam numerus propositus p, sicque ad residua omnium terminorum progressionis geometricae invenienda, non opus est operationem ultra terminum a^p continuare.

32. **Coroll. 5.** Si autem potestas a^λ sit minima earum, quae per numerum p divisae unitatem relinquunt, tunc quia singuli termini minores quam a^λ diversa praebent residua, in residuis omnibus, neque plures, neque pauciores diversi numeri occurrent quam λ. Igitur si λ sit minus quam $p - 1$, non omnes numeri in residuis occurrent: sed quidam numeri plane nunquam in divisione terminorum progressionis geometricae $1, a, a^2, a^3$, etc. remanere poterunt.

34. **Coroll. 6.** Si igitur diversitas residuorum spectetur, fieri potest, ut ex omnibus potestatibus ipsius a unicum tantum residuum vel duo tantum residua diversa, vel tria etc. prodeant, plura tamen nunquam, quam $p-1$, locum habere possunt. Quotquot autem prodierint residua, inter ea semper unitas reperitur.

35. **Theorema 9.** Si p sit numerus primus, et a primus ad p, atque omnes numeri ipso p minores reperiantur inter residua, quae ex divisione omnium potestatum ipsius a per numerum primum p oriuntur, tum a^{p-1} erit minima potestas, quae per p divisa unitatem relinquit.

Demonstratio. Sit a^λ minima potestas, quae per p divisa relinquat unitatem, atque ex praecedentibus patet, esse $\lambda < p$ (15). Jam cum numerus omnium residuorum diversorum sit $= \lambda$, et omnium numerorum ipso p minorum $= p - 1$, patet, si esset $\lambda < p - 1$, non omnes numeros minores quam p in residuis occurrere: non igitur erit $\lambda < p - 1$, neque vero est $\lambda > p - 1$, quia alioquin non foret $\lambda < p$. Unde relinquitur esse $\lambda = p - 1$. Quocirca si omnes numeri ipso p minores in residuis occurrant, potestas a^{p-1} erit minima, quae per p divisa unitatem relinquit.

36. **Scholion.** Natura hujus theorematis postulat, ut p sit numerus primus; nisi enim esset talis, fieri non posset, ut omnes numeri ipso p minores in residuis occurrerent. Quod quo clarius perspiciatur, perpendendum est, si p est numerus compositus, ad quem tamen a sit primus, nullam partem aliquotam ipsius p in residuis locum habere: nam si potestas quaepiam a^μ daret residuum r, quod esset pars aliquota ipsius p, ob $a^\mu = mp + r$, etiam ipsa potestas a^μ divisorem haberet r, ideoque nec ea, neque radix a esset numerus ad p primus, quod hypothesi adversatur.

37. **Theorema 10.** Si numerus diversorum residuorum, quae ex divisione potestatum $1, a, a^2, a^3, a^4, a^5$, etc. per numerum primum p nascuntur, minor sit quam $p-1$, tum ad minimum totidem erunt numeri, qui non sunt residua, quot sunt residua.

Demonstratio. Sit a^λ potestas minima, quae per p divisa unitatem relinquat, ac sit $\lambda < p - 1$, erit numerus omnium residuorum diversorum $= \lambda$, ideoque minor quam $p - 1$. Cum ergo numerus

omnium numerorum ipso p minorum, sit $= p - 1$, patet dari numeros in casu proposito, qui in residuis non locum obtineant. Dico autem hujusmodi numerorum numerum ad minimum esse $= \lambda$. Quod ut ostendatur, exponamus residua per ipsos terminos, ex quibus oriuntur, eruntque

$$\text{haec residua } 1, a, a^2, a^3, a^4 \ldots\ldots a^{\lambda-1}$$

quorum numerus $= \lambda$, atque haec residua, si ad formam consuetam reducantur, omnia erunt minora quam p et inter se diversa. Cum igitur sit $\lambda < p - 1$ per hypothesin, dabitur certe numerus, qui in his residuis non reperitur. Sit talis numerus k; jam dico si k non sit residuum, neque ak, neque a^2k, neque a^3k, etc. neque $a^{\lambda-1}k$ in residuis occurrere. Fac enim $a^\mu k$ esse residuum ex potestate a^α oriundum, foret $a^\alpha = np + a^\mu k$, seu $a^\alpha - a^\mu k = np$, ideoque

$$a^\alpha - a^\mu k = a^\mu (a^{\alpha-\mu} - k)$$

per p divisibile. At a^μ per p non est divisibile, esset ergo $a^{\alpha-\mu} - k$ per p divisibile, seu potestas $a^{\alpha-\mu}$ per p divisa, residuum relinqueret k, quod hypothesi repugnat. Ex quo patet, omnes hos numeros: $k, ak, a^2k, a^3k, a^4k, \ldots\ldots\ldots a^{\lambda-1}k$, seu numeros inde derivatos, non esse residua. At hi numeri, quorum multitudo $= \lambda$, omnes sunt diversi inter se; si enim duo, veluti $a^\mu k$ et $a^\nu k$, convenirent, ad idemque residuum r reducerentur, foret $a^\mu k = mp + r$ et $a^\nu k = np + r$, ideoque $a^\mu k - a^\nu k = (m - n)p$, seu $(a^\mu - a^\nu)k = (m - n)p$ esset per p divisibile. Neque vero k per p est divisibile, siquidem ponimus p numerum primum et $k < p$; esset $a^\mu - a^\nu$ per p divisibilis, seu $a^{\mu-\nu}$ per p divisum, unitatem relinqueret; cum tamen ob $\mu < \lambda - 1$ et $\nu < \lambda - 1$, esset $\mu - \nu < \lambda$, quod esset absurdum. Ergo omnes illi numeri $k, ak, a^2k, a^3k \ldots\ldots a^{\lambda-1}k$, si reducantur, erunt inter se diversi, eorumque multitudo est $= \lambda$. Ad minimum ergo dantur λ numeri, qui in residuis locum non inveniunt, siquidem sit $\lambda < p - 1$.

38. **Coroll. 1.** Cum igitur habeantur λ diversi numeri, qui sunt residua, totidemque diversi numeri, qui non sunt residua, omnesque sint minores quam p, illorum junctim sumtorum numerus 2λ major esse nequit, quam $p - 1$: quia non plures dantur numeri ipso p minores quam $p - 1$.

39. **Coroll. 2.** Si ergo a^λ sit minima potestas, quae per numerum primum p divisa relinquit unitatem, fueritque $\lambda < p - 1$, tum certum est, non esse $\lambda > \frac{p-1}{2}$, erit ergo vel $\lambda = \frac{p-1}{2}$, vel $\lambda < \frac{p-1}{2}$.

40. **Coroll. 3.** Ante vidimus exponentem istius posestatis minimae λ esse necessario minorem quam p; erit ergo vel $\lambda = p - 1$, vel $\lambda < p - 1$; hocque casu si $\lambda < p - 1$, simul novimus, jam esse vel $\lambda = \frac{p-1}{2}$, vel $\lambda < \frac{p-1}{2}$. Atque adeo intra limites $p - 1$ et $\frac{p-1}{2}$ nullus continetur numerus, qui unquam esse possit valor ipsius λ.

41. **Theorema 11.** Si p sit numerus primus, atque a^λ minima potestas ipsius a, quae per p divisa unitatem relinquit, fueritque $\lambda < \frac{p-1}{2}$, tum fieri nequit, ut iste exponens λ sit major quam $\frac{p-1}{3}$; eritque ergo vel $\lambda = \frac{p-1}{3}$, vel $\lambda < \frac{p-1}{3}$.

Demonstratio. Cum a^λ sit minima potestas, quae per numerum primum p divisa, unitatem relinquit, plures in residuis non occurrunt numeri diversi, quam λ, qui relinquuntur ex his terminis

$$1, a, a^2, a^3, a^4, \ldots\ldots a^{\lambda-1}$$

si singuli per p dividantur; quare cum sit $\lambda < p - 1$ habebuntur $p - 1 - \lambda$ numeri, qui non sunt residua, quorum si unus aliquis sit $= r$, vidimus hos omnes numeros

$$r,\ ar,\ a^2r,\ a^3r,\ a^4r\ .\ .\ .\ .\ .\ a^{\lambda-1}r$$

siquidem dividendo per p ad numeros ipso p minores reducantur, in residuis non contineri. Hinc autem tantum λ numeri ex residuis excluduntur; quare cum sit $\lambda < \frac{p-1}{2}$, erit $\lambda < p - 1 - \lambda$, ideoque praeter hos numeros alii insuper dantur, qui in residuis non continentur. Sit s hujusmodi numerus, qui neque sit residuum, neque in praecedente serie non residuorum contineatur; atque etiam hi omnes numeri

$$s,\ as,\ a^2s,\ a^3s,\ a^4s,\ .\ .\ .\ .\ .\ a^{\lambda-1}s$$

non erunt residua: hique numeri, uti in praecedente demonstratione ostendimus, omnes inter se erunt diversi. Neque vero ullus etiam horum numerorum, veluti $a^{\mu}s$, jam in praecedente serie non-residuorum continetur, seu non est $a^{\mu}s = a^{\nu}r$. Nam si esset $a^{\nu}r = a^{\mu}s$, foret $s = a^{\nu-\mu}r$, vel $s = a^{\lambda+\nu-\mu}r$, siquidem esset $\mu > \nu$, unde s jam in priori serie contineretur contra hypothesin. Quocirca si $\lambda < \frac{p-1}{2}$, dantur ad minimum adhuc λ numeri, qui non sunt residua, sique cum λ habeamus residua, et 2λ non-residua, hique numeri omnes sint ipso p minores, fieri nequit, ut sit eorum summa 3λ major quam $p - 1$, seu non erit $\lambda > \frac{p-1}{3}$. Erit ergo vel $\lambda = \frac{p-1}{3}$, vel $\lambda < \frac{p-1}{3}$, siquidem sit $\lambda < \frac{p-1}{2}$ et p numerus primus.

42. **Coroll. 1.** Si ergo non sit $\lambda < \frac{p-1}{3}$, tum certe erit $\lambda = \frac{p-1}{3}$, siquidem sit $\lambda < \frac{p-1}{2}$. At remota hac conditione, si noverimus non esse $\lambda < \frac{p-1}{3}$, tum necessario sequitur, esse vel $\lambda = \frac{p-1}{3}$, vel $\lambda = \frac{p-1}{2}$, vel $\lambda = p - 1$.

43. **Coroll. 2.** Sive autem sit $\lambda = \frac{p-1}{3}$, sive $\lambda = \frac{p-1}{2}$, potestas a^{p-1} per p divisa relinquit unitatem. Si enim a^{λ} unitatem relinquat, etiam $a^{2\lambda}$ et $a^{3\lambda}$ unitatem pro residuo dabunt.

44. **Theorema 12.** Si a^{λ} sit minima potestas ipsius a, quae per numerum primum p divisa unitatem relinquit, fueritque $\lambda < \frac{p-1}{3}$, tum certe non erit $\lambda > \frac{p-1}{4}$, eritque ergo vel $\lambda = \frac{p-1}{4}$, vel $\lambda < \frac{p-1}{4}$.

Demonstratio. Quia numerus omnium residuorum diversorum, quae ex divisione omnium potestatum ipsius a per numerum primum p proveniunt, est $= \lambda$, atque ex his terminis nascuntur $1,\ a,\ a^2,\ a^3,\ a^4\ .\ .\ .\ .\ .\ a^{\lambda-1}$: ob $\lambda < \frac{p-1}{3}$ habebuntur statim bis tot numeri, qui non sunt residua, qui ex his duabus progressionibus oriuntur

$$r,\ ar,\ a^2r,\ a^3r,\ a^4r\ .\ .\ .\ .\ .\ a^{\lambda-1}r$$
$$\text{et}\quad s,\ as,\ a^2s,\ a^3s,\ a^4s\ .\ .\ .\ .\ .\ a^{\lambda-1}s$$

horum numerorum, tam residuorum, quam non-residuorum numerus est $= 3\lambda$, ideoque minor quam $p - 1$, supererunt ergo adhuc numeri, qui non erunt residua. Sit t talis numerus, atque ut ante ostendimus, etiam hi omnes numeri

$$t,\ at,\ a^2t,\ a^3t,\ a^4t\ .\ .\ .\ .\ .\ .\ a^{\lambda-1}t$$

non erunt residua, quorum numerus est $=\lambda$. At hi numeri non solum inter se erunt diversi, cum p sit numerus primus, sed etiam a praecedentibus discrepant, sicque omnium horum numerorum, sive residuorum, sive non-residuorum multitudo est $=4\lambda$; et cum singuli hi numeri sint minores quam p, impossibile est, ut sit $4\lambda > p-1$; eritque ergo vel $\lambda = \frac{p-1}{4}$, vel $\lambda < \frac{p-1}{4}$; siquidem sit, ut assumsimus, $\lambda < \frac{p-1}{3}$ et p numerus primus.

45. **Coroll. 1.** Simili modo demonstrabitur, si sit $\lambda < \frac{p-1}{4}$; tum impossibile esse, ut sit $\lambda > \frac{p-1}{5}$, foreque idcirco vel $\lambda = \frac{p-1}{5}$, vel $\lambda < \frac{p-1}{5}$.

46. **Coroll. 2.** In genere etiam si constet esse $\lambda < \frac{p-1}{n}$, eodem modo demonstrabitur, fieri non posse, ut esset $\lambda > \frac{p-1}{n+1}$, eritque propterea vel $\lambda = \frac{p-1}{n+1}$, vel $\lambda < \frac{p-1}{n+1}$.

47. **Coroll. 3.** Hinc patet omnium numerorum, qui residua esse nequeant, numerum esse vel $=0$, vel $=\lambda$, vel $=2\lambda$, vel alii cuicunque multiplo ipsius λ: si enim plures fuerint istiusmodi numeri quam $n\lambda$, tum ob unicum statim λ novi insuper accedunt, ut eorum omnium numerus fiat $=(n+1)\lambda$; at si hic nondum omnes numeri non-residua contineantur, denuo subito λ novi accedent.

48. **Theorema 13.** Si p sit numerus primus, et a^λ minima potestas ipsius a, quae per p divisa unitatem relinquit, erit exponens λ divisor numeri $p-1$.

Demonstratio. Numerus ergo omnium residuorum diversorum est $=\lambda$, unde numerus reliquorum numerorum ipso p minorum, qui residua esse nequeunt, erit $=p-1-\lambda$, at hic numerus (47) est multiplum ipsius λ, puta $n\lambda$, ita ut sit $p-1-\lambda = n\lambda$, unde fit $\lambda = \frac{p-1}{n+1}$. Perspicuum ergo est, exponentem λ esse divisorem numeri $p-1$, unde si non sit $\lambda = p-1$, certe parti cuidam aliquotae numeri $p-1$ exponens λ aequalis erit.

49. **Theorema 14.** Si p sit numerus primus, et a primus ad p, tum potestas a^{p-1} per p divisa unitatem relinquet.

Demonstratio. Sit a^λ minima potestas ipsius a, quae per p divisa unitatem relinquit, erit, ut vidimus, $\lambda < p$, atque insuper demonstravimus, esse vel $\lambda = p-1$, vel λ esse partem aliquotam numeri $p-1$. Priori casu constat propositum, atque potestas a^{p-1} per p divisa unitatem relinquet. Posteriori casu, quo λ est pars aliquota numeri $p-1$, erit $p-1=n\lambda$, at cum potestas a^λ per p divisa unitatem relinquat, etiam omnes hae potestates $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$, etc. ideoque et $a^{n\lambda}$, seu a^{p-1}, per p divisae unitatem relinquent. Semper ergo potestas a^{p-1} per p divisa unitatem relinquit.

50. **Coroll. 1.** Quia potestas a^{p-1} per numerum primum p divisa unitatem relinquit, formula $a^{p-1}-1$ per numerum primum p erit divisibilis, siquidem a sit numerus ad p primus, seu si a non sit divisibilis per p.

51. **Coroll. 2.** Si ergo p sit numerus primus, omnes potestates exponentis $p-1$, veluti n^{p-1}, per p divisae, vel unitatem relinquent, vel nihil. Illud scilicet eveniet, si n sit numerus ad p primus, hoc vero si ipse numerus n per p fuerit divisibilis.

52. **Coroll. 3.** Si p sit numerus primus, atque numeri a et b primi ad p, erit differentia potestatum $a^{p-1} - b^{p-1}$ per numerum p divisibilis. Cum enim tam $a^{p-1} - 1$, quam $b^{p-1} - 1$, per p sit divisibilis, etiam differentia harum formularum, id est $a^{p-1} - b^{p-1}$, per p erit divisibilis.

53. **Scholion.** En ergo novam demonstrationem theorematis eximii, a Fermatio quondam prolati, quae maxime discrepat ab ea, quam in Comment. Acad. Petropol. Tomo VIII. dedi (*). Ibi enim evolutionem binomii $(a + b)^n$ in seriem modo Newtoniano in subsidium vocavi, quae consideratio a proposito non mediocriter abhorrere videtur; hic vero idem theorema ex solis potestatum proprietatibus demonstravi, unde haec demonstratio magis naturalis videtur, cum praeterea nobis alias insignes proprietates circa residua potestatum, quando per numeros primos dividuntur, manifestet. Patet etiam, si p sit numerus primus, non solum formulam $a^{p-1} - 1$ per p esse divisibilem, sed etiam interdum fieri posse, ut etiam forma simplicior $a^{\lambda} - 1$ per p sit divisibilis, tumque exponentem λ esse partem aliquotam exponentis $p - 1$.

54. **Theorema 15.** Si q sit numerus primus, atque potestas a^q per numerum primum p divisa unitatem relinquat, tum a^q erit minima potestas ipsius a, quae per p divisa unitatem relinquit, nisi forte ipse numerus a per p divisus unitatem relinquat.

Demonstratio. Sit enim a^{λ} minima potestas ipsius a, quae per numerum primum p divisa unitatem relinquat, atque nullae aliae potestates hac proprietate erunt praeditae, nisi $a^{2\lambda}$, $a^{3\lambda}$, $a^{4\lambda}$, etc. Verum nulli harum potestas a^q potest esse aequalis, nisi sit $\lambda = 1$, cum q sit numerus primus; ideoque necesse est, ut sit $q = \lambda$, ac perinde a^q minima potestas, quae per p divisa unitatem relinquit. Excipitur autem casus, quo $\lambda = 1$, seu quo ipse numerus a per p divisus unitatem relinquit: hoc enim casu omnis potestas a^n, sive ejus exponens n sit numerus primus, sive compositus, in divisione per p facienda unitatem relinquet.

55. **Coroll. 1.** Si ergo potestas a^q, cujus exponens est numerus primus, per numerum primum p divisa unitatem relinquat, tum q erit pars aliquota numeri $p - 1$, hocque casu formula $a^q - 1$ per numerum primum p erit divisibilis.

56. **Coroll. 2.** Cum q sit pars aliquota numeri $p - 1$, erit $p - 1 = nq$, et $p = nq + 1$. Quodsi ergo formula $a^q - 1$, in qua q est numerus primus, divisibilis sit per quempiam numerum primum p, habebit hic divisor semper hujusmodi formam $p = nq + 1$, nisi sit $p = a - 1$: nam $a - 1$ semper est divisor formulae $a^q - 1$.

57. **Coroll. 3.** Formula ergo $a^q - 1$, existente q numero primo, praeter divisorem $a - 1$ alios divisores primos non admittit, nisi qui in hac forma $nq + 1$ contineantur; et cum q sit numerus primus, ideoque impar, nisi sit $q = 2$, pro n nonnisi numeri pares capi possunt, eruntque ergo omnes divisores, si quos habet, in forma $2nq + 1$ contenti.

58. **Coroll. 4.** Quia igitur formulae $a^q - 1$ divisor est

$$a^{q-1} + a^{q-2} + a^{q-3} + a^{q-4} + \ldots\ldots + a^2 + a + 1$$

haec forma in $2nq + 1$ continebitur, eritque ergo haec expressio:

$$a^{q-1} + a^{q-2} + a^{q-3} + \ldots\ldots + a^2 + a$$

(*) Vide hujus operis comment. IV pag. 21. Conf. etiam comment. VII pag. 52.

per numerum primum q divisibilis, quicunque numerus sit a; at si $a = q$, vel $a = mq$, hoc est manifestum per se.

59. **Scholion 1.** Hoc etiam manifestum est, si a non sit vel q, vel mq; tum enim formula inventa abit in $a(a^{q-2} + a^{q-3} + a^{q-4} \ldots\ldots + a + 1)$, cujus factor posterior, qui transit in $\frac{a^{q-1}-1}{a-1}$, per q est divisibilis: quod quidem per se est evidens; nam cum q sit numerus primus, per eum formula $a^{q-1} - 1$ est divisibilis, eademque etiam per $a - 1$ divisa, manebit per q divisibilis, nisi $a - 1$ divisorem habeat q, qui casus jam ante est exceptus. Notandum enim est, formam

$$a^{q-1} + a^{q-2} + a^{q-3} \ldots\ldots + a^2 + a + 1$$

eatenus tantum in forma $2nq + 1$ contineri, quatenus illa est vel numerus primus, vel ex numeris primis ejusdem formae $2nq + 1$ compositus. At si illa formula ipsa jam habeat factorem $a - 1$, per quem forma $a^q - 1$ est divisibilis, tum ea cum forma $2nq + 1$ non conveniet. Sed si $a - 1 = mq$, vel $a = mq + 1$, tum ipsa illa formula per q erit divisibilis, quia terminorum numerus $= q$, neque ergo illa in forma $2nq + 1$ continebitur.

60. **Scholion 2.** Plurimum autem interest, nosse divisores formulae $a^q - 1$, quando q est numerus primus, quoniam ii alias, excepto divisore $a - 1$, qui sponte se prodit, difficillime investigantur, fierique adeo potest, ut saepe hujusmodi formula, postquam per $a - 1$ divisa, fiat numerus primus. At si q non est numerus primus, sed ipse divisores habeat m, n, tum manifesto erunt hae formulae $a^m - 1$ et $a^n - 1$ divisores formulae $a^q - 1$. His ergo casibus investigatio ulteriorum divisorum reducitur ad formulas $a^m - 1$ et $a^n - 1$, in quibus exponentes m et n sunt numeri primi. Novimus igitur, si quis tentando voluerit, divisores formulae $a^q - 1$ investigare, tentamen cum nullis aliis numeris primis, nisi qui in forma $2nq + 1$ contineantur, instituendum esse, quo ipso operatio alias difficillima non mediocriter contrahitur.

61. **Theorema 16.** Si potestas a^m, per numerum p divisa, residuum relinquat $= r$, tum etiam potestas $(a \pm \alpha p)^m$, per p divisa, idem relinquet residuum r.

Demonstratio. Si potestas $(a \pm \alpha p)^m$ evolvatur, prodibit

$$a^m \pm m\alpha a^{m-1} p + \frac{m(m-1)}{1 \cdot 2} \alpha^2 a^{m-2} p^2 \pm \text{etc.}$$

cujus omnes termini, praeter primum, per p sunt divisibiles: unde haec quantitas per p divisa idem relinquet residuum, ac si solus primus terminus a^m per p divideretur. Ergo cum potestas a^m residuum relinquat $= r$, etiam potestas $(a \pm \alpha p)^m$ residuum relinquet $= r$.

62. **Coroll. 1.** Si m sit numerus par, demonstratio etiam valet pro formula $(-a + \alpha p)^m$, hoc ergo casu etiam formula $(\alpha p - a)^m$, per p divisa, idem relinquit residuum r, quod formula a^m relinquit.

63. **Coroll. 2.** At si m sit numerus impar, quia formula $-a^m$ per p divisa residuum relinquit $= -r$, etiam formula $(\alpha p - a)^m$ residuum relinquet $= -r$.

64. **Theorema 17.** Si fuerit $a = c^n \pm \alpha p$, tum formula $a^{\frac{p-1}{n}}$, per numerum primum p divisa, unitatem relinquet, siquidem sit n divisor numeri $p - 1$.

Demonstratio. Cum sit $a = c^n \pm \alpha p$, potestas $a^{\frac{p-1}{n}}$, seu $(c^n \pm \alpha p)^{\frac{p-1}{n}}$ per p divisa, idem relinquit residuum, ac potestas $c^{n \cdot \frac{p-1}{n}}$, seu c^{p-1}, at ob p numerum primum, potestas c^{p-1} per p divisa unitatem relinquit, ergo etiam potestas $a^{\frac{p-1}{n}}$ unitatem relinquet, siquidem sit $a = c^n \pm \alpha p$, neque tamen a vel c divisibile fuerit per p.

65. **Coroll. 1.** Ex hoc ergo theoremate cognoscuntur casus, quibus potestates numerorum, quarum exponentes sunt minores quam $p-1$, si per numerum primum p dividantur, unitatem relinquunt.

66. **Coroll. 2.** Si ergo sit $a = cc \pm \alpha p$, existente p numero primo, tum potestas $a^{\frac{p-1}{2}}$ per p divisa unitatem relinquet, seu formula $a^{\frac{p-1}{2}} - 1$ per p erit divisibilis. Cum autem p sit numerus primus, nisi sit $= 2$, semper exponens $\frac{p-1}{2}$ erit numerus integer.

67. **Coroll. 3.** Si sit $a = c^3 \pm \alpha p$, tum potestas $a^{\frac{p-1}{3}}$ per p divisa unitatem relinquet, seu haec forma $a^{\frac{p-1}{3}} - 1$ per p erit divisibilis. Hic casus locum habet, si numerus primus p ita sit comparatus, ut $p-1$ per 3 sit divisibile.

68. **Theorema. 18.** Si sit $ab^n = c^n \pm \alpha p$, et p numerus primus, tum potestas $a^{\frac{p-1}{n}}$ per p divisa unitatem relinquet, siquidem $\frac{p-1}{n}$ fuerit numerus integer.

Demonstratio. Potestas $(c^n \pm \alpha p)^{\frac{p-1}{n}}$, seu $a^{\frac{p-1}{n}} b^{p-1}$, per p divisa idem relinquit residuum, quod potestas $c^{n \cdot \frac{p-1}{n}} = c^{p-1}$, ac haec potestas unitatem relinquit, ergo et potestas $a^{\frac{p-1}{n}} b^{p-1}$. Hujus autem factor b^{p-1} pariter unitatem relinquit; ergo necesse est, alterum quoque factorem $a^{\frac{p-1}{n}}$, si per p dividatur, unitatem relinquere, nisi sit b vel c divisibile per p.

69. **Coroll. 1.** Si ergo sit $ab^n = c^n \pm \alpha p$, seu $ab^n - c^n$, sive $c^n - ab^n$, per numerum primum p divisibile, tum haec quoque formula $a^{\frac{p-1}{n}} - 1$ per p erit divisibilis.

70. **Coroll. 2.** Cum p sit numerus primus, ponatur $p = mn + 1$, atque si fuerit haec formula $ab^n - c^n$, seu $c^n - ab^n$, per p divisibilis, tum etiam haec formula $a^m - 1$ per numerum primum p erit divisibilis.

71. **Coroll. 3.** Dummodo ergo pro b et c ejusmodi numeri dentur, ut $ab^n - c^n$, seu $c^n - ab^n$ divisionem per numerum primum $p = mn + 1$ admittat, tum certum est, hanc formulam $a^m - 1$ per eundem numerum primum $p = mn + 1$ esse divisibilem.

72. **Theorema 19.** Si formula $a^m - 1$ fuerit divisibilis per numerum primum $p = mn + 1$, tum semper dantur numeri x et y ejusmodi, ut $ax^n - y^n$ sit per euudem numerum primum p divisibilis.

Demonstratio. Cum enim x^{mn} et y^{mn} per p divisae unitatem relinquant, formula $a^m x^{mn} - y^{mn}$ semper erit per p divisibilis, dummodo neque x, neque y per p sit divisibile. Cum jam per factores sit

$$a^m x^{mn} - y^{mn} = (ax^n - y^n)(a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}y^n + a^{m-3}x^{mn-3n}y^{2n} + \ldots + y^{mn-n})$$

si quis neget factorem primum $ax^n - y^n$ unquam esse per p divisibilem, is affirmare cogitur, alterum factorem semper esse per p divisibilem, dummodo pro x et y non capiantur numeri per p divisibiles. Retineat x valorem quemcunque, at pro y ponamus successive numeros 1, 2, 3, 4, usque ad $p - 1 = mn$, ne unquam obtineat valorem per p divisibilem, sitque brevitatis gratia

$$A = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n} + \ldots + 1$$
$$B = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}2^n + \ldots + 2^{mn-n}$$
$$C = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}3^n + \ldots + 3^{mn-n}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$N = a^{m-1}x^{mn-n} + a^{m-2}x^{mn-2n}(mn)^n + \ldots + (mn)^{mn-n}$$

ac forent omnes hae quantitates $A, B, C, \ldots. N$, quae progressionem algebraicam ordinis $mn - n$ constituunt, per p divisibiles, hincque etiam earum differentiae primae, secundae, tertiae et ordinis cujusvis. At hujus seriei differentia ordinis $mn - n$, quae tantum per terminos $mn - n + 1$ seriei definitur, neque adeo terminum $(mn + 1)^{mn-n}$, seu p^{mn-n} involvit, quia p non potest esse valor ipsius y, est uti constat:

$$1.\ 2.\ 3.\ 4.\ 5.\ \ldots\ldots\ (mn - n)$$

quae aperte non est per numerum primum $p = mn + 1$ divisibilis, quia nullos alios habet divisores primos, nisi qui sint minores quam $mn - n$. Cum igitur haec differentia ordinis $mn - n$ non sit divisibilis per p, sequitur non omnes terminos seriei $A, B, C, D, \ldots. N$ esse per p divisibiles. Illo igitur casu, vel illis casibus ipsius y, quibus termini hujus seriei non sunt per p divisibiles, necessario alter factor $ax^n - y^n$ per p erit divisibilis.

73. **Coroll. 1.** Quicunque ergo numerus pro x sumatur, modo per p non divisibilis, pro y semper datur valor $< p$, qui reddit formulam $ax^n - y^n$ per p divisibilem. Similique modo, si pro y numerus pro lubitu assumatur, demonstrari potest, semper pro x ejusmodi numerum $< p$ inveniri posse, quo eadem formula per p divisibilis evadat.

74. **Coroll. 2.** Si ergo $a^m - 1$ fuerit divisibile per numerum primum $mn + 1 = p$, atque pro x capiatur numerus quicunque b per p non divisibilis, semper inveniri potest numerus y, ut haec forma $ab^n - y^n$, seu $y^n - ab^n$, fiat per $p = mn + 1$ divisibilis.

75. **Coroll. 3.** Simili modo si forma $a^m - 1$ fuerit divisibilis per numerum primum $p = mn + 1$, atque pro y capiatur numerus quicunque c, per p non divisibilis, semper inveniri poterit numerus x, ut haec forma $ax^n - c^n$, seu $c^n - ax^n$, fiat per $p = mn + 1$ divisibilis.

76. **Theorema 20.** Si haec forma $ab^n - c^n$, vel $c^n - ab^n$, fuerit divisibilis per numerum primum $p = mn + 1$, tum sumto numero d pro lubitu, dummodo per p non sit divisibilis, semper inveniri potest numerus x, ut vel haec forma $ax^n - d^n$, vel haec $ad^n - x^n$, vel $d^n - ax^n$, vel $x^n - ad^n$ fiat per eundem numerum primum $p = mn + 1$ divisibilis.

Demonstratio. Cum haec forma $ab^n - c^n$, vel $c^n - ab^n$ sit per numerum primum $p = mn + 1$ divisibilis, tum etiam hic numerus $a^m - 1$ per eundem numerum primum $p = mn + 1$ erit divisibilis

(71). Verum si $a^m - 1$ per p est divisibilis, sumto numero quocunque d per p non divisibili, dabitur numerus x, ut vel haec forma $ax^n - d^n$, vel etiam haec $ad^n - x^n$, vel $d^n - ax^n$, vel $x^n - ad^n$ fiat quoque per numerum primum $p = mn + 1$ divisibilis.

77. **Corollarium.** Posito ergo $d = 1$, si formulae $ab^n - c^n$ divisor sit numerus primus $p = mn + 1$, tum dabitur numerus x, ut vel haec forma $ax^n - 1$, vel $a - x^n$, vel $x^n - a$ fiat per eundem numerum primum p divisibilis.

78. **Scholion.** Theorema undevicesimum, quod inversum est theorematis duodevicesimi, jam alibi proposueram (*), sed sine demonstratione, et tametsi tum ejus demonstrationem multis modis tentavi, eam tamen invenire non potui, donec in methodum hic usitatam incidi: quae igitur eo magis notatu digna videtur, cum dubium sit nullum, quin eadem ad multa alia numerorum arcana viam sit patefactura. Haec quoque methodus, quae in consideratione differentiarum continetur, nuper mihi insigni usui fuit, dum ejus beneficio tandem pulcherrimi theorematis Fermatiani, quo omnis numerus primus formae $4n + 1$ aggregatum duorum quadratorum esse affirmatur, demonstrationem sum consecutus (**), ad quam ante nullo alio modo pervenire potui.

(*) Vide pag. 60. 61. (**) Vide partem priorem comment. XV pag. 210 — 215. Conf. etiam pag. 163.

XX.

Theoremata arithmetica nova methodo demonstrata.

(N. Comment. VIII. 1760—61. p. 74. Exhib. 1759 Oct. 15.)

Praeter varias computandi operationes, quae vulgo in arithmetica tradi solent, hujusque disciplinae quasi partem practicam constituunt, ejusdem pars theoretica, quae in indaganda numerorum natura versatur, non minus jam olim tractari est coepta, quemadmodum ex Euclide et Diophanto intelligere licet, ubi insignes numerorum proprietates erutae reperiuntur ac demonstratae. Quo magis autem deinceps numerorum indolem et affectiones mathematici sunt scrutati, multo plures eorum proprietates observaverunt, unde pulcherrima theoremata numerorum naturam illustrantia derivavere, quae partim demonstrationibus sunt munita, partim etiam nunc iis indigent, sive quod eae ab auctoribus non sint inventae, sive temporum injuria deperditae: ex quo genere plurima passim occurrunt hujusmodi theoremata numerica, quorum demonstrationes adhuc desiderantur, etiamsi eorum veritatem in dubium vocare non liceat. Atque hic insigne discrimen, quod inter theoremata arithmetica et geometrica intercedit, non parum mirari debemus, quod vix ulla propositio geometrica proferri possit, quam non sit in promtu, sive veram, sive falsam, ostendere, dum contra multae circa numerorum naturam notae sunt propositiones, quarum veritatem nobis agnoscere, neutiquam vero demonstrare liceat. Magna hujusmodi theorematum copia a Fermatio relicta habetur, quorum demonstrationes maximam partem se invenisse affirmavit, quas cum ejus scriptis interiisse in eximium hujus scientiae detrimentum non parum est dolendum. Quot autem talium theorematum demonstrationes vel sunt cognitae, vel restitutae, in iis certe multo major vis ingenii elucet, quam vix in ullo alio demonstrationum genere deprehendimus; unde in hoc negotio non tam utilitas, qua scientia numerorum illustratur, est aestimanda, quam maxima subtilitas, qua hujusmodi demonstrationes prae aliis distinguuntur. Atque ob hanc causam, cum jam saepius, quam plerisque aequum videri queat, in hoc genere laboraverim, operam mihi equidem non perdidisse videor, neque etiam nunc theoremata, quae hic propono, utilitate caritura confido. Notatu imprimis dignum visum est theorema illud Fermatii, quo omnes numeros in hac formula $a^{p-1}-1$ contentos, semper divisibiles esse per numerum p, siquidem is fuerit primus, neque tamen a per eum divisionem admittat, affirmavit, cujus theorematis jam geminam dedi demonstrationem (*). Nunc autem idem in latiori sensu contemplor, atque in genere, si divisor non sit numerus primus, sed quicunque N, investigo, cujusmodi exponentem potestati cuicunque tribui oporteat, ut expressio a^n-1 semper sit divisibilis per numerum N, dummodo numerus a cum eo nullum habeat divisorem communem. Inveni autem hoc

(*) Conf. pagg. 21. 52.

semper usu venire, quoties exponens n aequalis fuerit multitudini numerorum ipso N minorum, qui sint ad N primi. Ad hoc ergo demonstrandum, ante omnia hujusmodi theorematibus est opus, ex quibus, proposito numero quocunque N, cognosci possit, quot inter numeros ipso minores futuri sint ad eum primi, seu qui nullum cum eo habeant communem divisorem; quae theoremata jam ipsa, multo ampliorem usum habere, atque ad alias magis absconditas numerorum proprietates aditum parere videntur. Iis autem praemissis, demonstratio veritatis propositae ita est comparata, ut majore attentione non indigna videatur.

1. **Theorema 1.** Si per numerum quemcunque n termini progressionis arithmeticae cujuscunque, cujus differentia sit numerus ad n primus, dividantur, inter residua occurrent omnes numeri divisore n minores.

Demonstratio. Sit progressionis arithmeticae terminus primus $= a$, et differentia $= d$, quae sit ad n numerus primus, seu quae cum numero n nullum praeter unitatem habeat divisorem communem, ita ut progressio arithmetica futura sit:

$$a,\ a+d,\ a+2d,\ a+3d,\ a+4d,\ a+5d,\ \text{etc.}$$

ac dico: si singuli termini per numerum n dividantur, inter residua omnes numeros ipso n minores occurrere. Ad hoc demonstrandum sufficiet hujus progressionis tantum n terminos considerasse, qui sunt:

$$a,\ a+d,\ a+2d,\ a+3d,\ \ldots\ a+(n-1)d.$$

Quodsi ergo isti termini singuli per n dividantur, omnia residua inter se diversa esse oportet. Si enim duo termini, veluti $a+\mu d$ et $a+\nu d$, existentibus μ et ν numeris ipso n minoribus, per n divisi paria praeberent residua, eorum differentia $(\nu-\mu)d$ utique per n esset divisibilis. Cum autem numeri d et n nullum habeant divisorem communem, necesse esset, ut $\nu-\mu$ divisionem per n admitteret; id quod esset absurdum, ob $\nu-\mu<n$. Quare cum omnia illa residua sint diversa, eorumque numerus, utpote terminorum numero aequalis, sit $=n$, in iis omnes plane numeri ipso n minores occurrent, scilicet:

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ \ldots\ldots\ (n-1)$$

siquidem differentia progressionis d sit numerus ad divisorem propositum n primus. Q. E. D.

2. **Coroll. 1.** Inter terminos ergo progressionis arithmeticae cujuscunque, quorum numerus est n, dummodo differentia ejus ad n sit numerus primus, certe reperitur unus, qui per n est divisibilis: tum vero etiam aderit unus, qui per n divisus datum residuum r relinquit.

3. **Coroll. 2.** Si ergo numerus d ad n fuerit primus, semper numerus hujus formae $a+\nu d$ exhiberi potest, existente a numero quocunque et ν minore quam n, qui per numerum n sit divisibilis, atque etiam sub iisdem conditionibus semper talis dabitur numerus $a+\nu d$, qui per n divisus datum relinquat residuum r.

4. **Coroll. 3.** Datis igitur numeris a et d, quorum hic d ad n sit primus, semper invenire licet numeros μ et ν, ut aequationi huic: $a+\nu d=\mu n$, vel etiam huic: $a+\nu d=\mu n+r$ satisfiat, quicunque numerus minor quam n pro r assumatur.

5. **Scholion.** Quod de progressionis arithmeticae terminorum numero n demonstravimus, id de tota progressione in infinitum continuata valet: termini enim, qui post illos n terminos sequuntur,

eadem ordine reproducunt residua, si per n dividantur. Ita terminorum post $a+(n-1)d$ sequentium, qui sunt $a+nd$, $a+(n+1)d$, $a+(n+2)d$, etc. per n divisorum residua, conveniunt cum residuis ex terminis initialibus a, $a+d$, $a+2d$, etc. natis. Atque si tota series in infinitas periodos distribuatur, cuique n terminos tribuendo, hoc modo:

$$a,\ a+d \ldots a+(n-1)d \mid a+nd \ldots a+(2n-1)d \mid a+2nd \ldots a+(3n-1)d \mid$$

termini cujuslibet periodi eadem praebebunt residua, eodemque ordine disposita; omnium enim periodorum termini cum primi, tum secundi, et tertii etc. constanter paria dabunt residua. Quare si rationem residuorum cognoscere velimus, sufficit unicam periodum examinasse.

6. **Theorema 2.** In progressione arithmetica, cujus terminorum numerus est $=n$, totidem termini erunt ad numerum n primi, quot inter numeros ipso n minores dantur ad n primi, dummodo differentia progressionis fuerit ad n numerus primus.

Demonstratio. Sit enim a terminus primus, et d differentia progressionis, quae sit ad n numerus primus, ideoque ipsa progressio n continens terminos:

$$a,\ a+d,\ a+2d,\ a+3d,\ \ldots\ldots\ a+(n-1)d.$$

Quoniam igitur, si hi termini per numerum n dividantur, inter residua occurrunt omnes plane numeri ipso n minores, ponamus ex termino quocunque $a+\nu d$ resultare residuum r, ac manifestum est, si r fuerit numerus ad n primus, illum quoque terminum $a+\nu d$ ad n fore primum; sin autem r cum n habeat quempiam divisorem communem, idem quoque erit divisor communis numerorum n et $a+\nu d$. Quare quot inter numeros ipso n minores fuerint numeri ad n primi, totidem quoque inter terminos progressionis arithmeticae propositae habebuntur numeri ad n primi. Q. E. D.

7. **Coroll. 1.** Si n fuerit numerus primus, quia omnes numeri, ipso minores, ad ipsum quoque sunt primi, quorum numerus ergo est $=n-1$; in illa etiam progressione arithmetica omnes termini praeter unum erunt ad n primi, quippe unus per n est divisibilis.

8. **Coroll. 2.** Sin autem n fuerit numerus compositus, inter numeros ipso minores dabuntur quipiam, qui cum eo divisorem habeant communem; totidemque vero etiam reperientur in progressione arithmetica, quibus iidem communes divisores cum n conveniant.

9. **Coroll. 3.** Ita si sit $n=6$, quia inter numeros senario minores sunt duo ad 6 primi, scilicet 1 et 5; in omni progressione arithmetica 6 terminorum:

$$a,\ a+d,\ a+2d,\ a+3d,\ a+4d,\ a+5d$$

duo tantum erunt ad 6 primi, dummodo differentia d sit ad 6 numerus primus. Ita si capiatur $a=4$; $d=5$, horum sex numerorum 4, 9, 14, 19, 24, 29, duo, scilicet 19 et 29, ad 6 sunt primi, unus 24 per 6 divisibilis, reliqui vero 4, 9, 14 ad 6 compositi perinde ac 2, 3, 4.

10. **Scholion.** Haec theoremata in doctrina et contemplatione naturae numerorum insignem habent usum, hic autem ea solum adhibere visum est ad hanc quaestionem enodandam: *Proposito numero quocunque* n, *quot inter numeros ipso minores futuri sint ad eundem numerum* n *primi?* Statim quidem patet si n sit numerus primus, omnes numeros ipso minores simul ad eum fore primos, eorumque idcirco numerum esse $=n-1$. Verum si n sit numerus compositus, multitudo numerorum ipso minorum ad eumque primorum est minor; quanta autem sit quovis casu, non tam

facile assignari potest. Ita si sit $n = 12$, inter numeros minores tantum quatuor reperiuntur ad 12 primi, scilicet 1, 5, 7, 11: et si sit $n = 60$, numeri minores ad eum primi sunt:

$$1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59,$$

quorum numerus est 16: unde reliqui 43 omnes cum 60 divisores habent communes. Moneri hic convenit, unitatem ad omnes plane numeros esse numerum primum, etiamsi omnium sit divisor; id quod ex definitione est evidens, qua numeri dicuntur esse inter se primi, qui praeter unitatem alium nullum agnoscunt divisorem.

11. **Theorema 3.** Si n sit potestas quaecunque numeri primi p, seu $n = p^m$, inter numeros ipso minores tot erunt ad eum primi, quot unitates continentur in $p^m - p^{m-1} = p^{m-1}(p - 1)$.

Demonstratio. Multitudo omnium numerorum potestate $n = p^m$ minorum est $p^m - 1$; inter hos autem reperiuntur quidam, qui ad n non sunt primi, omnia scilicet ipsius p multipla, minora quam n, nullique alii praeterea: ex quo sequentes numeri ad n non erunt primi:

$$p, 2p, 3p, 4p \ldots\ldots p^m - p,$$

quorum numerus est $p^{m-1} - 1$; quo ablato a numero omnium ipso $n = p^m$ minorum, relinquitur multitudo eorum, qui ad p^m sunt primi, quorum numerus itaque est $= p^m - p^{m-1} = p^{m-1}(p - 1)$. Q. E. D.

12. **Coroll. 1.** Hinc igitur primo sequitur, id quod per se est manifestum, si sit $n = p$, existente p numero primo, numerum omnium numerorum ipso minorum ad eumque primorum esse $= p - 1$, siquidem omnes numeri ipso minores simul sunt ad eum primi.

13. **Coroll. 2.** At si sit $n = p^2$, inter numeros ipso minores, multitudo eorum, qui ad eum sunt primi, est $= pp - p = p(p - 1)$; reliqui, quorum numerus est $p - 1$, ad $n = p^2$ erunt compositi, seu per p divisibiles.

14. **Coroll. 3.** Proposita autem numeri primi potestate quacunque $n = p^m$, inter numeros ipso minores, quorum multitudo est $= p^m - 1$, reperiuntur $p^{m-1} - 1$, qui sunt per p divisibiles, ideoque ad p^m non primi: reliqui vero omnes, quorum numerus est $= p^m - p^{m-1} = p^{m-1}(p - 1)$ ad p^m sunt primi.

15. **Scholion.** Si ergo numerus propositus n fuerit potestas cujuspiam numeri primi, ope hujus regulae assignare poterimus, quot inter omnes numeros ipso minores futuri sint ad eum primi. Quando autem numerus n, ex duobus pluribusve numeris primis fuerit conflatus, hinc nondum ista quaestio confici potest: praecedentibus autem theorematibus adhibendis istam quaestionem latius patentem resolvere poterimus.

16. **Theorema 4.** Si numerus n sit productum duorum numerorum primorum p et q, seu $n = pq$, multitudo omnium numerorum ipso minorum ad eumque primorum est $= (p - 1)(q - 1)$.

Demonstratio. Cum numerus omnium numerorum ipso $n = pq$ minorum sit $pq - 1$, hinc primum ii debent excludi, qui per p sunt divisibiles, deinde vero etiam ii, qui per q, hisque deletis

relinquetur multitudo quaesita. Notentur ergo ab unitate usque ad pq numeri, qui sunt ad p primi, hoc modo:

$$\begin{array}{ccccc} 1, & 2, & 3, & 4, & \ldots\ p-1 \\ p+1, & p+2, & p+3, & p+4 & \ldots\ 2p-1 \\ 2p+1, & 2p+2, & 2p+3, & 2p+4 & \ldots\ 3p-1 \\ 3p+1, & 3p+2, & 3p+3, & 3p+4 & \ldots\ 4p-1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (q-1)p+1, & (q-1)p+2, & (q-1)p+3, & (q-1)p+4 & \ldots\ pq-1 \end{array}$$

atque jam ex his ii tantum eligi debent, qui simul quoque ad q sunt primi. Considerentur ergo series verticales, quarum numerus est $p-1$; quaelibet autem continet q terminos in arithmetica progressione crescentes, differentia existente p, quae est ad q numerus primus. In qualibet ergo serie verticali omnes termini, praeter unum, ad q erunt primi (per § 7); unde unaquaeque series verticalis continet $q-1$ numeros ad q primos. Quare cum numerus serierum verticalium sit $p-1$, in omnibus continentur simul $(p-1)(q-1)$ numeri ad q primi, iidemque igitur etiam ad productum pq erunt primi; consequenter inter omnes numeros ipso pq minores reperientur $(p-1)(q-1)$ numeri ad pq primi. Q. E. D.

17. **Coroll. 1.** Cum multitudo omnium numerorum ipso producto pq minorum sit $pq-1$, inter eos semper sunt $(p-1)(q-1) = pq-p-q+1$ primi ad pq, reliqui vero, quorum numerus est $p+q-2$, ad eum sunt compositi, seu cum eo communem habent divisorem vel p, vel q.

18. **Coroll. 2.** Hoc etiam inde patet, quod inter numeros ipso producto pq minores sint $q-1$ numeri per p divisibiles, scilicet:

$$p,\ 2p,\ 3p,\ 4p\ \ldots\ (q-1)p$$

deinde inter eosdem sunt $p-1$ numeri per q divisibiles, nempe:

$$q,\ 2q,\ 3q,\ 4q\ \ldots\ (p-1)q$$

qui cum ab illis omnes sint diversi, omnino habentur $(q-1)+(p-1) = p+q-2$ numeri, qui ad pq non sunt primi.

19. **Coroll. 3.** Si ergo quaeratur, quot ab 1 usque ad 15 sint numeri ad 15 primi? ob $p=3$ et $q=5$, regula docet eorum numerum esse $2.4=8$, quippe qui sunt 1, 2, 4, 7, 8, 11, 13, 14. Simili modo ab 1 ad 35 ob $p=5$ et $q=7$, multitudo numerorum ad 35 primorum est $4.6=24$, hique numeri sunt:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

20. **Scholion.** Quoniam hic quaestio est de numeris, qui ad quempiam numerum sint primi, eoque minores, eos commode partes ad istum numerum primas appellare licebit. Ita si numerus propositus fuerit primus $=p$, numerus partium ad eum primarum est $=p-1$: si numerus propositus sit potestas quaecunque numeri primi $=p^n$, numerus partium ad eum primarum erit

$$=p^n-p^{n-1}=p^{n-1}(p-1):$$

at si numerus propositus sit productum duorum numerorum minorum disparium $=pq$, numerus

partium ad eum primarum est $= (p-1)(q-1)$, hocque modo ambages in loquendo contrahemus. Simili modo demonstrare possemus, si numerus propositus sit productum ex tribus numeris primis disparibus $= pqr$, numerum partium ad eum primarum fore $= (p-1)(q-1)(r-1)$: hocque adeo ad productum plurium extendere liceret. Verum sequens propositio omnes hos casus in se complectetur.

21. **Theorema 5.** Si sint A et B numeri inter se primi, et numerus partium ad A primarum sit $= a$, numerus vero partium ad B primarum sit $= b$; tum numerus partium ad productum AB primarum erit $= ab$.

Demonstratio. Sint $1, \alpha, \beta, \gamma, \ldots \omega$ numeri illi ipso A minores ad eumque primi, seu partes ad A primae, quarum igitur partium numerus per hypothesin est $= a$. Totidem ergo erunt numeri ad A, itidem primi erunt ab A ad $2A$, item a $2A$ ad $3A$, et ita porro. Hoc modo exhiberi poterunt omnes numeri ad A primi ab unitate usque ad numerum propositum AB, quos sequens schema exhibebit:

$$\begin{array}{cccc}
1, & \alpha, & \beta, \;\ldots & \omega \\
A+1, & A+\alpha, & A+\beta, \;\ldots & A+\omega \\
2A+1, & 2A+\alpha, & 2A+\beta, \;\ldots & 2A+\omega \\
3A+1, & 3A+\alpha, & 3A+\beta, \;\ldots & 3A+\omega \\
\ldots & \ldots & \ldots & \ldots \\
(B-1)A+1, & (B-1)A+\alpha, & (B-1)A+\beta, \;\ldots & (B-1)A+\omega.
\end{array}$$

Hic singulae series horizontales continent a terminos, numerusque omnium serierum horizontalium est $= B$; unde omnes series junctim offerunt aB terminos, qui jam omnes ad A erunt primi. Inde ergo adhuc excludi debent ii, qui ad B non sunt primi, ut hoc modo relinquantur, qui non solum ad A, sed etiam ad B, ideoque ad ipsum productum AB, sint primi, seu ex his seriebus ii tantum termini numerari debent, qui etiam ad B sint primi. Hunc in finem consideremus series verticaliter; et cum numerus serierum verticalium sit $= a$, quaelibet series verticalis continebit B terminos in arithmetica progressione auctos, quorum differentia cum sit $= A$, ideoque numerus ad B primus, per theorema 2 quaelibet series verticalis tot continebit terminos ad B primos, quot dantur partes ad numerum B primae; eorum ergo numerus est per hypothesin $= b$. Cum igitur singulae series verticales contineant b terminos ad B primos, qui propterea etiam erunt ad productum AB primi, numerus omnium terminorum ad AB primorum, hoc est partium ad hunc numerum AB primarum erit $= ab$. Q. E. D.

22. **Coroll. 1.** Si insuper tertius numerus C adjiciatur, qui sit ad utrumque praecedentium A et B, seu ad eorum productum AB primus, et numerus partium ad C primarum sit $= c$; tum numerus partium ad productum ABC primarum erit $= abc$. Productum enim AB considerari potest tanquam unus numerus, cujus partium ad eum primarum numerus sit $= ab$; et quia C ad AB est primus, theorema hic habet locum.

23. **Coroll. 2.** Cum igitur unusquisque numerus N resolvi possit in factores inter se primos, qui singuli sint vel ipsi numeri primi, vel potestates primorum, ope hujus regulae multitudo partium ad numerum quemcunque N primarum assignari poterit.

24. **Coroll. 3.** Existentibus scilicet p, q, r, s, etc. numeris primis, omnis numerus N in hujusmodi forma $N = p^{\lambda}, q^{\mu}, r^{\nu}, s^{\xi}$ comprehendetur, unde numerus partium ad N primarum erit:

$$p^{\lambda-1}(p-1),\quad q^{\mu-1}(q-1),\quad r^{\nu-1}(r-1),\quad s^{\xi-1}(s-1).$$

25. **Coroll. 4.** Pro formis igitur numerorum simplicioribus multitudo partium ad eos primarum ita se habebit:

numerus propositus	multitudo partium ad eum primarum
p	$p-1$
pp	$p(p-1)$
pq	$(p-1)(q-1)$
p^3	$pp(p-1)$
p^2q	$p(p-1)(q-1)$
pqr	$(p-1)(q-1)(r-1)$
p^4	$p^3(p-1)$
p^3q	$p^2(p-1)(q-1)$
p^2q^2	$p(p-1)q(q-1)$
p^2qr	$p(p-1)(q-1)(r-1)$
$pqrs$	$(p-1)(q-1)(r-1)(s-1)$
p^5	$p^4(p-1)$
p^4q	$p^3(p-1)(q-1)$
p^3q^2	$p^2(p-1)q(q-1)$
p^3qr	$p^2(p-1)(q-1)(r-1)$
p^2q^2r	$p(p-1)q(q-1)(r-1)$
p^2qrs	$p(p-1)(q-1)(r-1)(s-1)$
$pqrst$	$(p-1)(q-1)(r-1)(s-1)(t-1)$

num. prop.	mult. part. ad eum prim.
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8
21	12
22	10
23	22
24	8
25	20

26. **Coroll. 5.** Hinc igitur proposito numero quocunque multitudo partium ad eum primarum expedite definietur. Veluti, si proponatur 360, cum sit $360 = 2^3 . 3^2 . 5$, erit multitudo partium ad 360 primarum $= 4 . 6 . 4 = 96$.

27. **Scholion.** Haec circa multitudinem partium ad numerum quemvis primarum pro praesenti instituto sufficere possunt. Interim tamen circa ipsas partes ad quemvis numerum primas haec notasse juvabit: si numerus propositus fuerit N, atque inter partes ad eum primas occurrat numerus α, ibidem quoque occurret numerus $N-\alpha$; quoniam, existente α ad N primo, etiam $N-\alpha$ erit ad N primus. Hinc pro quovis numero partes tantum ejus semisse minores invenisse sufficiet, cum reliquae sint earum complementa ad ipsum numerum N. Simili modo, si N sit numerus par, inter partes ad N primas etiam occurret $\frac{1}{2}N-\alpha$, tum etiam $\frac{1}{2}N+\alpha$. Item si N sit divisibilis per

numerum quemcunque n, inter partes ad eum primas quoque occurrent hi numeri:

$$\frac{1}{n}N \pm a;\quad \frac{2}{n}N \pm a;\quad \frac{3}{n}N \pm a \ldots\ldots \frac{(n-1)}{n}N \pm a \quad \text{et} \quad N - a$$

hincque multo facilius ipsae partes istae actu exhiberi poterunt.

28. **Theorema 6.** Si numerus x fuerit primus ad N, tum omnes potestates ipsius x per N divisae relinquent residua, quae erunt ad numerum N prima.

Demonstratio. Cum enim x sit numerus ad N primus, omnes ejus potestates erunt quoque ad N primae, ideoque si per N dividantur, residua etiam ad N erunt numeri primi. Q. E. D.

29. **Coroll. 1.** Inter residua ergo potestatum ipsius x per N divisarum alii numeri non occurrunt, nisi qui sint partes ad N primae; quarum numerus cum sit pro indole numeri N determinatus, innumerabiles existent potestates ipsius x, quae per N divisae aequalia relinquunt residua.

30. **Coroll. 2.** Inter residua autem ista ex divisione potestatum ipsius x per numerum N orta semper reperietur unitas, propterea quod inter potestates ipsius x etiam referri debet $x^0 = 1$. Utrum autem praeter unitatem etiam omnes reliquae partes ad N primae inter residua occurrant, nec ne? mox videbimus.

31. **Coroll. 3.** Si pro x capiatur unitas, omnia residua erunt unitates, quicunque numerus pro N fuerit assumtus. Deinde si sumatur $x = N - 1$, qui numerus ad N etiam est primus, in residuis, ex divisione potestatum $(N-1)^0$, $(N-1)^1$, $(N-1)^2$, $(N-1)^3$, etc. ortis, nonnisi duo reperientur diversa, scilicet 1 et $N - 1$, quae continuo se alternatim excipiunt.

32. **Coroll. 4.** Prout igitur numerus x ratione ad N fuerit comparatus, utique fieri potest, ut inter residua omnium potestatum ipsius x non omnes partes ad divisorem N primae occurrant.

33. **Coroll. 5.** Si ergo omnes partes ad numerum N primae sint $1, a, b, c, d, e, \ldots$ quarum numerus sit $= n$, inter residua memorata, vel omnes istae partes occurrent, vel quaedam tantum, inter quas autem semper unitas reperietur.

34. **Coroll. 6.** Quodsi non omnes illae partes in residuis ex divisione potestatum ipsius x per numerum N relictis occurrant, illae partes in duas classes distribuentur, quarum altera continebit partes in residuis occurrentes, altera vero partes in residuis non occurrentes.

35. **Theorema 7.** Si series potestatum x^0, x^1, x^2, x^3, x^4, x^5, etc. per numerum N, qui ad x sit primus, dividatur, eousque residua prodibunt diversa, donec perveniatur ad potestatem, quae iterum unitatem pro residuo praebeat.

Demonstratio. Quoniam serie potestatum $1, x, x^2, x^3, x^4$, etc. in infinitum continuata, omnia residua diversa esse nequeunt, necesse est, ut tandem quodpiam ex praecedentibus residuis redeat; ac dico: unitatem esse id residuum, quod omnium primum sit rediturum. Quod si quis neget, sit x^μ ea potestas, cujus residuum primum in sequentibus ex potestate $x^{\mu+\nu}$ redeat; cum igitur potestates x^μ et $x^{\mu+\nu}$ aequalia praebeant residua, earum differentia $x^{\mu+\nu} - x^\mu = x^\mu(x^\nu - 1)$ per numerum N erit divisibilis. Verum producti $x^\mu(x^\nu - 1)$ factor prior ad N est numerus primus, ergo alter $x^\nu - 1$ per N divisibilis sit necesse est. Hinc autem potestas x^ν per N divisa residuum daret $= 1$, sicque unitas inter sequentia residua citius redibit, quam residuum potestatis x^μ, quippe

quod per hypothesin demum in potestate altiore $x^{\mu+\nu}$ recurrit. Ex quo evidens, nullum residuum iterum occurrere posse, nisi ante unitas inter residua redierit. Q. E. D.

36. **Coroll. 1.** Postquam divisio terminorum seriei $1, x, x^2, x^3, x^4$, etc. per numerum N ad x primum ab initio dedit residua diversa, puta $1, \alpha, \beta, \gamma$, etc. tandem iterum occurret primum residuum 1; quod si oriatur ex potestate x^ν, numerus praecedentium residuorum diversorum erit $= \nu$.

37. **Coroll. 2.** Quando autem potestas x^ν residuum dat 1, idem quod primus terminus x^0, potestas sequens $x^{\nu+1}$ idem dabit residuum quod x^1; et sequentium quaecunque $x^{\nu+\mu}$ idem quod potestas x^μ. Cum enim differentia $x^{\nu+\mu} - x^\mu = x^\mu(x^\nu - 1)$ sit divisibilis per N, necesse est, ut ambo termini $x^{\nu+\mu}$ et x^μ per N divisi idem praebeant residuum.

38. **Coroll. 3.** Cum post potestatem x^ν eadem residua $1, \alpha, \beta, \gamma$, etc. ordine recurrant, potestas $x^{2\nu}$, similique modo post eam potestates $x^{3\nu}, x^{4\nu}, x^{5\nu}$, etc. omnes per N divisae idem residuum 1 relinquent. Quin etiam omnes potestates $x^\mu, x^{\mu+\nu}, x^{\mu+2\nu}, x^{\mu+3\nu}, x^{\mu+4\nu}$, etc. aequalia residua suppeditabunt.

39. **Coroll. 4.** Si igitur x^ν fuerit infima potestas, quae post $x^0 = 1$ iterum unitatem pro residuo praebeat, numerus diversorum residuorum erit ν. Cum ergo numerus partium ad numerum N primarum sit $= n$, fieri certe nequit, ut sit $\nu > n$: erit ergo vel $\nu = n$, vel $\nu < n$.

40. **Coroll. 5.** Si ergo series potestatum $1, x, x^2, x^3$, etc. usque ad x^n continuetur, inter eas certe una saltem reperietur praeter primum terminum 1, quae per N divisa unitatem relinquat. Plures fortasse hujusmodi potestates aliquando, sed pauciores una nunquam existent.

41. **Scholion.** Residua proprie semper sunt numeri minores divisore N, sed nihil impedit, quo minus numeros etiam majores tanquam residua spectemus, cujusmodi relinquuntur, si quotus nimis parvus accipiatur. Ita si in divisione cujuspiam numeri per N relinquatur $N + \alpha$, hoc residuum aequivalens ipsi α censeri debet; hincque, si de residuis sermo sit, omnes hi numeri α, $N + \alpha$, $2N + \alpha$, $3N + \alpha$ etc. instar unius residui α sunt considerandi. Scilicet multipla quaecunque divisoris N sive adjecta, sive demta a quopiam residuo α, ejus naturam non mutant, atque hoc modo etiam numeri negativi commode inter residua referuntur; veluti $\alpha - N$ pro eodem residuo est habendum ac α; et residuum -1 aequivalet residuo $N - 1$. Ex his conficitur, omnes numeros, qui per N divisi idem exhibeant residuum α, pro eodem residuo haberi posse, ex quo enim numero per divisionem, quotum nimis parvum sumendo, oritur residuum vel $N + \alpha$, vel $2N + \alpha$, vel $3N + \alpha$ etc. ex eodem, quotum plenum sumendo, nascitur residuum α; tum vero indidem, si quotus capiatur nimis magnus, obtinebuntur residua negativa $\alpha - N$, vel $\alpha - 2N$, vel $\alpha - 3N$ etc. quae ergo etiam ab α non discrepare sunt censenda.

42. **Theorema. 8.** Si dum termini progressionis $1, x, x^2, x^3, x^4$, etc. per numerum N ad x primum dividantur, residua fuerint $1, a, b, c$, etc., in iisdem quoque occurrent tam singulorum omnes potestates, quam producta quaecunque vel binorum, vel ternorum, vel quotlibet in se multiplicatorum.

Demonstratio. Nascantur residua a, b, c, etc. ex potestatibus $x^\alpha, x^\beta, x^\gamma$, etc. ac numeros etiam majores quam N in residuis admittendo, ex potestatibus $x^{2\alpha}, x^{3\alpha}, x^{4\alpha}$, etc. orientur residua

a^2, a^3, a^4, etc. quae igitur etiam in serie residuorum 1, a, b, c, etc. continebuntur. Tum vero potestates $x^{\alpha+\beta}$, $x^{\alpha+\gamma}$, $x^{\alpha+\beta+\gamma}$, etc. relinquent residua ab, ac, abc, etc. quae ergo etiam in serie residuorum inveniri debebunt. Producta igitur, quomodocunque ex residuis 1, a, b, c, etc. per multiplicationem formata, omnia in eadem serie residuorum occurrent, si quidem singula per ablationem divisoris N, quoties id fieri potest, ad minimam formam reducantur. Q. E. D.

43. **Coroll. 1.** Haec indoles residuorum eo clarius eluceret, si eorum loco ipsae illae potestates ipsius x, unde sunt orta, substituantur; tum enim manifesto non solum omnes potestates harum potestatum, sed etiam earum producta quaecunque in residuis occurrunt.

44. **Coroll. 2.** Neque tamen ideo numerus residuorum indeterminatus evadit; quemadmodum enim jam vidimus, ex innumeris potestatibus paria residua provenire, ita, si omnia haec residua, ex mutua multiplicatione nata, ad formam minimam reducantur, ad multitudinem modicam revocabuntur.

45. **Coroll. 3.** Ita si minima potestas, quae per N divisa iterum unitatem relinquit, fuerit x, ita ut numerus residuorum 1, a, b, c, etc. sit $=\nu$, tum in eodem numero omnia producta, ex multiplicatione numerorum a, b, c, etc. nata, continebuntur, si quidem ab iis divisor N toties, quoties fieri potest, auferatur.

46. **Scholion.** Unicum exemplum omnibus dubiis, quae forte circa hanc apparentem residuorum multitudinem nasci possunt, solvendis sufficiet. Sit igitur $x=2$, et pro divisore sumatur $N=15$ qui scilicet ad 2 sit primus, jam singulae binarii potestates per 15 divisae, sequentia relinquent residua

potestates:	1,	2,	2^2,	2^3,	2^4,	2^5,	2^6,	2^7,	2^8,	2^9,	2^{10},	etc.
residua:	1,	2,	4,	8,	1,	2,	4,	8,	1,	2,	4,	etc.

Potestas igitur, quae primum unitatem reproducit, est 2^4, a qua residua continuo eodem ordine 1, 2, 4, 8 repetuntur, ita ut tantum quaterna residua diversa occurrant. Hic jam manifestum est, quomodocunque haec residua in se invicem multiplicentur, nunquam numeros inde produci, qui non in eodem quaternione includantur, postquam scilicet ablatione divisoris 15 ad formam minimam fuerint revocata. In hoc quoque exemplo inter residua non omnes partes ad 15 primae occurrunt, sed inde excluduntur istae partes 7, 11, 13, 14, quae pariter ad 15 sunt primae; unde distributio supra facta inter partes ad divisorem primas, quae in residuis occurrunt, et quae non occurrunt, illustratur, ad quam potissimum in sequentibus probe respiciatur.

47. **Theorema 9.** In residuis ex divisione potestatum cujuspiam numeri per divisorem ad eum primum relictis, vel omnes partes ad divisorem primae occurrunt, vel numerus partium non occurrentium aequalis erit, vel rationem tenebit multiplam ad numerum partium, quae residua constituunt.

Demonstratio. Sit series potestatum 1, x, x^2, x^3, x^4, x^5, etc. et divisor N ad x primus, cujus partium ad ipsum primarum numerus sit $=n$. Sit porro x^ν minima potestas, quae per N divisa iterum unitatem relinquit, ita ut numerus omnium diversorum residuorum sit $=\nu$, quae cum omnia sint ad N numeri primi, eorum numerus erit vel $=n$, vel minor; priorique casu inter residua

utique omnes partes ad N primae occurrent. Consideremus igitur casum, quo $\nu < n$, sintque 1, a, b, c, d, etc. omnia residua ex divisione potestatum

$$1, x, x^2, x^3, x^4 \ldots\ldots x^{\nu-1}$$

per divisorem N relicta, quorum numerus cum sit $= \nu$, non omnes partes ad N primae ibi occurrent. Sit igitur α hujusmodi pars in residuis non occurrens, ac demonstrari potest, nullum quoque horum numerorum αa, αb, αc, αd etc. in residuis occurrere. Nam si αa esset residuum potestati x^λ respondens, quia a est quoque residuum ex quapiam potestate, puta x^ξ, ortum, foret

$$x^\lambda = AN + \alpha a \quad \text{et} \quad x^\xi = BN + a,$$

ideoque $x^\lambda - \alpha x^\xi = (A - \alpha B)N$ per N divisibile. Cum autem x^ξ ad N sit numerus primus, et $x^\lambda - \alpha x^\xi = x^\xi(x^{\lambda-\xi} - \alpha)$, numerus $x^{\lambda-\xi} - \alpha$ esset per N divisibilis, sicque potestas $x^{\lambda-\xi}$ per N divisa relinqueret residuum α, contra hypothesin. Cum igitur α, αa, αb, αc, etc. quorum numerus est $= \nu$, sint numeri ad N primi, atque divisione per N ad partes ad N primas revocari possint, statim atque una pars α ad N prima in residuis non reperitur, simul quoque ν ejusmodi partes assignari possunt in residuis non occurrentes. Numerus ergo partium non occurrentium, nisi sit nullus, ad minimum est $= \nu$, ac si praeterea fuerit pars ad N prima β in his non-residuis non contenta, denuo habebuntur ν partes novae in residuis non occurrentes; sicque porro. Quare si non omnes partes ad divisorem N primae in residuis occurrant, numerus partium non occurrentium necessario est vel $= \nu$, vel $= 2\nu$, vel $= 3\nu$, vel alii cuipiam multiplo ipsius ν, hoc est numeri diversorum residuorum. Q. E. D.

48. **Coroll. 1.** Constituto ergo discrimine inter partes ad divisorem N primas, eas quae sunt residua, et eas quae non sunt residua, ex demonstratione patet, productum ex residuo et non-residuo in classe non-residuorum semper contineri. Ita si a sit residuum, α non-residuum, productum αa certe non erit residuum.

49. **Coroll. 2.** Contra autem jam supra vidimus productum ex duobus pluribusve residuis in classe residuorum reperiri. Unde sequitur productum ex uno non-residuo et quotcunque residuis in classe non-residuorum occurrere debere.

50. **Scholion.** Vis hujus demonstrationis isto nititur fundamento, quod si inter residua occurrant partes 1, a, b, c, d, etc. ad divisorem primae, atque α fuerit etiam pars ad divisorem prima in his residuis non contenta, tum producta omnia αa, αb, αc, αd, etc. non solum in residuis non occurrere, quod quidem perfecte est demonstratum, sed etiam ea esse partes ad divisorem N primas, omnesque inter se diversas; seu si ea per N actu dividantur, relinqui residua diversa. Illud quidem per se est perspicuum: cum enim tam α, quam a, b, c, d, etc. sint numeri ad N primi, etiam eorum producta ad N prima sint necesse est. Quod autem producta αa, αb, αc, αd, etc. sint omnia ad N relata inter se diversa, intelligitur, quod si verbi gratia duo αa et αb per N divisa paria darent residua, eorum differentia $\alpha b - \alpha a = \alpha(b - a)$ per N esset divisibilis, ideoque et $b - a$; id quod hypothesi, quod a et b sint diversae partes ad N primae, repugnat.

51. **Theorema 10.** Exponens minimae potestatis x^ν, quae per numerum N ad x primum divisa unitatem relinquit, vel est aequalis numero partium ad N primarum, vel hujus numeri semissis, aliave ejus pars aliquota.

Demonstratio. Sit n numerus partium ad N primarum, quarum cum ν constituant residua, erit numerus non-residuorum $= n - \nu$. Vidimus autem hunc numerum esse vel $= 0$, vel $= \nu$, vel $= 2\nu$, vel alii cuipiam multiplo exponentis ν. Sit ergo $n - \nu = (m - 1)\nu$, ita ut m denotet vel unitatem, vel alium quemvis numerum integrum, atque hinc obtinebimus $n = m\nu$ et $\nu = \frac{n}{m}$: unde patet exponentem minimae potestatis ipsius x, quae per N divisa unitatem relinquit, esse vel $= n$, si $m = 1$, vel $= \frac{n}{2}$, si $m = 2$, vel in genere esse partem quampiam aliquotam numeri n, qui exprimit multitudinem partium ad divisorem N primarum. Q. E. D.

52. **Coroll. 1.** Si x^ν fuerit minima potestas, quae per numerum N ad x primum divisa unitatem relinquit, sequentes potestates idem residuum relinquentes sunt $x^{2\nu}$, $x^{3\nu}$, $x^{4\nu}$, $x^{5\nu}$, etc. neque praeterea ullae aliae dantur, quae per N divisae unitatem relinquant.

53. **Coroll. 2.** Exponens ergo hujus potestatis minimae semper cum numero partium ad divisorem N primarum ita connectitur, ut sit vel illi ipsi, vel cuipiam ejus parti aliquotae, aequalis.

54. **Scholion.** Quo haec ratio clarius perspiciatur, juvabit nonnullos casus simpliciores perpendisse. Sit igitur $x = 2$, et pro N sumamus successive numeros impares, utpote ad $x = 2$ primos, atque exhibeamus minimam potestatem binarii, quae per quemque numerum imparem divisa unitatem relinquat.

Divisor N	num. part. ad eum pr. n	min. pot. 2^ν quae per N divisa unitatem relinquit.		
3	2	2^2	ergo	$\nu = n$
5	4	2^4	—	$\nu = n$
7	6	2^3	—	$\nu = \frac{1}{2}n$
9	6	2^6	—	$\nu = n$
11	10	2^{10}	—	$\nu = n$
13	12	2^{12}	—	$\nu = n$
15	8	2^4	—	$\nu = \frac{1}{2}n$
17	16	2^8	—	$\nu = \frac{1}{2}n$
19	18	2^{18}	—	$\nu = n$
21	12	2^6	—	$\nu = \frac{1}{2}n$
23	22	2^{11}	—	$\nu = \frac{1}{2}n$
25	20	2^{20}	—	$\nu = n$
27	18	2^{18}	—	$\nu = n$
29	28	2^{28}	—	$\nu = n$
31	30	2^5	—	$\nu = \frac{1}{6}n$

55. **Theorema 11.** Si fuerit N ad x numerus primus, et n numerus partium ad N primarum, tum potestas x^n unitate minuta semper per numerum N erit divisibilis.

Demonstratio. Sit enim x^ν minima potestas, quae per N divisa unitatem relinquit, eritque ν vel aequalis ipsi numero n, vel parti ejus cuipiam aliquotae $\frac{n}{m}$. Cum igitur $x^\nu - 1$ per N sit divisibilis, quia forma $x^{\nu m} - 1$ factorem habet $x^\nu - 1$, etiam ista forma $x^{\nu m} - 1$, seu $x^n - 1$, per N erit divisibilis. Q. E. D.

56. **Coroll. 1.** Si ergo divisor N sit numerus primus p, neque x per p sit divisibilis, tum semper numerus $x^{p-1} - 1$ per numerum primum p erit divisibilis, uti quidem dudum demonstravi.

57. **Coroll. 2.** Si praeterea p, q, r, etc. sint numeri primi, x neque ullum eorum implicet, ex hoc theoremate sequitur,

has formas	fore divisibiles per
$x^{p-1} - 1$	p
$x^{p(p-1)} - 1$	pp
$x^{(p-1)(q-1)} - 1$	pq
$x^{pp(p-1)} - 1$	p^3
$x^{p(p-1)(q-1)} - 1$	ppq
$x^{(p-1)(q-1)(r-1)} - 1$	pqr

58. **Coroll. 3.** Si x et y sint primi ad divisorem N, cujus partium ad eum primarum numerus sit $= n$, quia tam $x^n - 1$, quam $y^n - 1$, est divisibilis per N, erit etiam $x^n - y^n$ semper divisibilis per numerum N, quod est theorema generalius.

59. **Coroll. 4.** Proposito ergo numero quocunque N, cujus partium ad ipsum primarum numerus sit $= n$, quicunque numerus ad N primus pro x capiatur, formula $x^n - 1$ semper erit per numerum N divisibilis.

60. **Coroll. 5.** Saepenumero vero etiam evenire potest, ut hujusmodi formula simplicior, veluti $x^{\frac{1}{2}n} - 1$, vel $x^{\frac{1}{3}n} - 1$, vel $x^{\frac{1}{4}n} - 1$, etc. sit per numerum N divisibilis, quae circumstantia pendet a certa indole numeri x.

61. **Scholion.** En ergo novam demonstrationem theorematis Fermatiani, quod si fuerit p numerus primus, omnes numeri in hac forma $a^{p-1} - 1$ contenti sint per p divisibiles, dummodo numerus a non sit per p divisibilis. Duas autem jam dudum hujus theorematis dederam demonstrationes; sed ea quam hic exhibui, iis praestare videtur, quod non solum ad numeros primos adstringitur. Quicunque enim numerus N pro divisore accipiatur, dummodo a ad eum sit primus, hic numerus $a^n - 1$ semper per N erit divisibilis, siquidem n denotet numerum partium ad N primarum, quae propositio multo latius patet, quam Fermatiana. Ex quo eo magis utilitas theorematum primorum elucet, quibus numerum partium ad quemque numerum primarum definivi, quae sine hac applicatione nimis sterilia videri potuissent.

XXI.

Supplementum quorundam theorematum arithmeticorum, quae in nonnullis demonstrationibus supponuntur.

(N. Comment. VIII. 1760—61. p. 105. Exhib. 1759. Oct. 15.)

Cum nuper demonstravissem, non dari duos cubos, quorum summa sit cubus, sine sufficiente probatione assumseram, omnes numeros in hac forma contentos $mm + mn + nn$, quae forma facile ad hanc reducitur: $pp + 3qq$, nunquam alios admittere divisores, nisi qui ipsi in eadem forma contineantur. Atque hinc conclusi, si forma $mm + mn + nn$ fuerit cubus, aliave potestas, ejus radicem quoque numerum ejusdem formae esse futuram; cui fundamento etiam tota demonstratio modo memorata innititur(*). Cum deinceps methodum novam et maxime generalem exposuissem, tres cubos inveniendi, quorum summa sit cubus, quae simul omnibus adhuc usitatis facilitate longe praestabat(**), non solum eandem indolem numerorum, in forma $mm + mn + nn$, seu $pp + 3qq$, contentorum, tanquam certam assumsi, sed etiam in evolutione solutionis supposui, hujus generis numeros alios divisores primos, praeter ternarium, non implicare, nisi qui essent formae $6x + 1$. Quin etiam vicissim affirmare licet, omnes numeros primos istius formae $6x + 1$, cujusmodi sunt 7, 13, 19, 31, 37, 43, etc. ita esse comparatos, ut in forma $pp + 3qq$ contineantur(***): veluti

$$7 = 2^2 + 3.1^2, \quad 13 = 1^2 + 3.2^2, \quad 19 = 4^2 + 3.1^2, \quad 31 = 2^2 + 3.3^2, \text{ etc.}$$

Quae theoremata, etsi jam a Fermatio fuerant prolata, nusquam tamen adhuc demonstrata reperiuntur: ex quo operae pretium me facturum putavi, si has assertiones rigidis demonstrationibus confirmarem, quo simul supra memoratae demonstrationes ad summum certitudinis gradum eveherentur.

His proprietatibus innituntur ratiocinia, quibus sum deductus, ad tres cubos, quorum summa itidem est cubus, hinc autem omissis ratiociniis solutio consueto modo adornari poterit, idoneis formis pro radicibus cuborum assumendis. Quarum ratio etsi non perspiciatur, tamen in hoc analyseos genere problemata plerumque per hujusmodi formulas feliciter excogitatas resolvi solent, in quas saepenumero, vel casu, vel post plurima tentamina incidimus.

Ita si tres cubi inveniri debeant, quorum summa sit cubus, positis eorum radicibus x, y et z, statuatur

$$x^3 + y^3 + z^3 = v^3.$$

Tum vero istorum cuborum radicibus sequentes formae tribuantur:

$$x = (m - n)p + qq; \qquad z = pp - (m + n)q$$
$$y = (m + n)p - qq, \qquad v = pp + (m - n)q$$

et quoniam loco quaternarum quantitatum x, y, z et v, quaternae novae m, n, p et q in calculum

(*) ? (**) Vide pag. 198 seqq. (***) Vide pag. 188, nec non pag. 35 theor. 7 et 8.

introducuntur, his positionibus problema non restringi est censendum. Cum igitur vi problematis esse oporteat

$$x^3 + y^3 = v^3 - z^3, \quad \text{sive}$$

$$(x + y)(xx - xy + yy) = (v - z)(vv + vz + zz)$$

per assumtas formas habebitur:

$$x + y = 2mp, \quad xx - xy + yy = (mm + 3nn)pp - 6npqq + 3q^4$$
$$v - z = 2mq, \quad vv + vz + zz = 3p^4 - 6nppq + (mm + 3nn)qq$$

hisque valoribus substitutis obtinebitur, divisione utrinque per $2m$ facta:

$$(mm + 3nn)p^3 - 6nppqq + 3pq^4 = 3p^4q - 6nppqq + (mm + 3nn)q^3,$$

ubi cum termini medii se utrinque destruant, fiet

$$(mm + 3nn)(p^3 - q^3) = 3p^4q - 3pq^4 = 3pq(p^3 - q^3).$$

Hic igitur commodo usu venit, ut haec aequatio per $p^3 - q^3$ dividi queat, in quo ipso summa utilitas nostrarum positionum consistit; nanciscimur enim hanc aequationem

$$mm + 3nn = 3pq$$

unde assumtis numeris m et n cum altero reliquorum p vel q pro lubitu, alter sponte et quidem rationaliter determinatur, quod eximium commodum non locum haberet, nisi postrema aequatio divisionem per $p^3 - q^3$ admisisset. Nisi ergo fractiones evitare velimus, habebimus statim

$$q = \frac{mm + 3nn}{3p}.$$

Verum etsi fractiones facile erui possunt, dum aeque multipla quaecunque radicum x, y, z et v pariter satisfaciunt, tamen ad expressiones simpliciores pertingemus, si numeros m et n statim ita assumamus, ut $mm + 3nn$ primo divisibile evadat per 3, tum vero insuper duos contineat factores, quorum alter pro p, alter pro q accipi queat.

Primo igitur statuatur $m = 3k$, ut fiat $pq = nn + 3kk$, et quia, ut mox demonstrabo, numeri formae $nn + 3kk$ alios non admittunt divisores, nisi qui ipsi sint ejusdem formae, ponamus:

$$nn + 3kk = (aa + 3bb)(cc + 3dd)$$

ut sit: $\qquad p = aa + 3bb \quad \text{et} \quad q = cc + 3dd,$

eritque $\qquad$ vel $n = ac + 3bd, \quad k = bc - ad, \quad m = 3bc - 3ad,$

$\qquad\qquad$ vel $n = ac - 3bd, \quad k = bc + ad, \quad m = 3bc + 3ad.$

Hanc pluralitatem valorum per ambiguitatem signorum ita exhibere poterimus, ut sit

$$m = \pm 3(bc \pm ad), \quad n = \pm(ac \mp 3bd)$$

ideoque diversi valores pro m et n, sumtis pro a, b, c, d numeris quibuscunque, erunt

I. $m + n = 3(bc + ad) + (ac - 3bd), \quad m - n = 3(bc + ad) - (ac - 3bd),$

II. $m + n = 3(bc + ad) - (ac - 3bd), \quad m - n = 3(bc + ad) + (ac - 3bd),$

III. $m + n = 3(bc - ad) + (ac + 3bd), \quad m - n = 3(bc - ad) - (ac + 3bd),$

IV. $m + n = 3(bc - ad) - (ac + 3bd), \quad m - n = 3(bc - ad) + (ac + 3bd).$

Hinc autem sequuntur solutiones, quas jam dudum fusius exposui, quare ad propositum revertor, sequentes propositiones demonstraturus.

1. **Propositio 1.** Si numeri a et b non sint numeri inter se primi, tum numerus $aa + 3bb$ non erit primus, sed divisibilis erit per quadratum maximi communis divisoris numerorum a et b.

Demonstratio. Sit enim m maximus communis divisor numerorum a et b, ita ut sit $a = mc$ et $b = md$, existentibus jam c et d numeris inter se primis, quia alioquin non esset maximus communis divisor. Ac numerus $aa + 3bb$ induet hanc formam: $mm(cc + 3dd)$, quae propterea certo divisorem habet mm.

2. **Coroll. 1.** Nisi ergo numeri a et b sint primi inter se, numerus ex iis formatus $aa + 3bb$ primus esse nequit. Neque vero hinc vicissim concludere licet, numerum $aa + 3bb$ semper esse primum, quoties numeri a ei b fuerint primi inter se.

3. **Coroll. 2.** Primo autem patet, numerum $aa + 3bb$ divisibilem esse per ternarium, dum numerus a fuerit multiplum ternarii, etiamsi caeterum a et b fuerint numeri primi inter se. Neque vero unquam forma $aa + 3bb$ per 9 altioremve ternarii potestatem est divisibilis, nisi ambo numeri a et b communem divisorem habeant 3.

4. **Coroll. 3.** Deinde etiam patet, formam $aa + 3bb$ numerum parem esse non posse, nisi ambo numeri a et b vel sint pares, vel impares. Utroque autem casu numerus $aa + 3bb$ non solum per 2, sed etiam per 4 erit divisibilis.

5. **Coroll. 4.** Non ergo datur numerus formae $aa + 3bb$, qui sit impariter par, sed statim atque admittit divisorem 2, simul erit divisibilis per 4. Unde quoties hujusmodi numeri fuerint pares, quaternarium, tanquam eorum factorem simplicem, considerare licet, etiamsi alias quaternarius, utpote binarii quadratum, non inter numeros primos referatur.

6. **Coroll. 5.** Si ergo numerus formae $aa + 3bb$ sit primus, non solum certo constat, ambos numeros a et b esse primos inter se, sed etiam utrumque non esse imparem. Necesse igitur est, ut alter sit par, alter vero impar.

7. **Propositio 2.** Si numerus formae $aa + 3bb$ per ternarium est divisibilis, tunc etiam quotus est numerus formae ejusdem.

Demonstratio. Si numerus $aa + 3bb$ per 3 est divisibilis, necesse est, ut radix prioris quadrati a sit multiplum ternarii. Ponamus ergo $a = 3c$, et numerus propositus erit $9cc + 3bb$, qui per 3 divisus dat quotum $3cc + bb$, qui utique est numerus ejusdem formae $aa + 3bb$.

8. **Scholion.** Notari hic convenit ipsum quoque ternarium esse numerum formae $aa + 3bb$, quippe qui prodit, si $a = 0$ et $b = 1$. Consideramus autem has duas formas

$$aa + 3bb \quad \text{et} \quad mm + mn + nn$$

tanquam aequivalentes, quoniam posterior in priorem transit, ponendo $m = a + b$, et $n = b - a$; unde quicquid de altera demonstramus, etiam de altera valet. Posterior autem, casu $m = 1$ et $n = 1$, manifesto dat 3. Videtur quidem forma $mm + mn + nn$, si numerorum m et n alter fuerit par, alter impar, ad priorem reduci non posse, quia tum in integris esse nequit $m = a + b$ et $n = b - a$; verum dantur adhuc aliae reductiones, scilicet $a = \frac{1}{2}m + n$, et $b = m$, sive $a = m + \frac{1}{2}n$,

et $b = n$, quarum ope, si numerorum m et n alter fuerit par, alter impar, forma $mm + mn + nn$ ad $aa + 3bb$ reducitur.

9. **Propositio 3.** Si numerus formae $aa + 3bb$ per quaternarium est divisibilis, tum etiam quotus erit numerus ejusdem formae $aa + 3bb$.

Demonstratio. Divisio formae $aa + 3bb$ per 4 succedit, si vel uterque numerorum a et b fuerit par, vel impar. Priori casu ponatur $a = 2c$, et $b = 2d$, fietque $aa + 3bb = 4cc + 12dd$, unde, divisione per 4 instituta, prodit quotus $cc + 3dd$.

Sin autem uterque numerus a et b fuerit impar, tum eorum vel summa, vel differentia, certo erit divisibilis per 4. Namque, cum tam $a + b$, quam $a - b$ sit numerus par, eorumque summa sit $2a$, hoc est numerus impariter par, necesse est, ut alter eorum sit impariter par, alter vero pariter par. Erit ergo, vel $a + b = 4c$, vel $a - b = 4c$, ideoque $a = 4c \pm b$: quo valore substituto fiet

$$aa + 3bb = 16cc \pm 8bc + 4bb$$

unde, divisione per 4 instituta, prodit quotus

$$4cc \pm 2bc + bb = (b \pm c)^2 + 3cc.$$

10. **Coroll. 1.** Hic pariter notasse juvabit, ipsum quaternarium etiam esse numerum formae $aa + 3bb$, inde resultantem, positis $a = 1$, et $b = 1$. At ex forma $mm + mn + nn$ quaternarius nascitur, si ponatur $n = 0$ et $m = 2$.

11. **Coroll. 2.** Cum igitur viderimus, dari numeros formae $aa + 3bb$, qui tam per 3, quam per 4, sint divisibiles: nunc demonstravimus, quotos ex utraque divisione resultantes etiam esse numeros ejusdem formae $aa + 3bb$.

12. **Coroll. 3.** Quodsi autem ambo numeri a et b fuerint impares, tum quotus, ex divisione numeri $aa + 3bb$ per 4 nascens, erit numerus impar. Vidimus enim, quotum esse $4cc \pm 2bc + bb$, qui, ob b numerum imparem, certo est impar.

13. **Scholion.** Quod hactenus de divisione numerorum formae $aa + 3bb$ per 3 et 4 demonstravimus, idem demonstrabimus de divisione per numerum quemcunque alium primum formae $aa + 3bb$; quotum scilicet inde oriundum pariter fore numerum ejusdem formae. Hunc in finem, ut brevitati consulamus, denotabunt litterae P, Q, R, S, etc. numeros primos formae $aa + 3bb$, inter quos tamen etiam quaternarium referemus, etiamsi non sit primus, propterea quod binarius ab hac forma est excludendus.

14. **Propositio 4.** Si numerus formae $aa + 3bb$ est divisibilis per numerum primum $P = pp + 3qq$, tum quotus est etiam numerus ejusdem formae.

Demonstratio. Si $aa + 3bb$ est divisibilis per $pp + 3qq$, tum etiam $aapp + 3bbpp$ per eundem est divisibilis, itemque $aapp + 3aaqq$; quare etiam horum numerorum differentia $3aaqq - 3bbpp$, ideoque et $aaqq - bbpp = (aq + bp)(aq - bp)$. Cum igitur $pp + 3qq$ sit numerus primus, necesse est, ut alteruter istorum factorum, scilicet vel $aq + bp$, vel $aq - bp$, sit per $pp + 3qq$ divisibilis. Ponatur ergo pro utroque casu $aq \pm bp = m(pp + 3qq)$: hincque fiet

$$a = \frac{m(pp + 3qq)}{q} \pm \frac{bp}{q} = 3mq + \frac{p}{q}(mp \pm b).$$

Verum quia a est numerus integer, et p et q numeri inter se primi, necesse est, ut $mp \mp b$ divisionem per q admittat. Ponatur ergo $mp \mp b = \mp nq$, eritque

$$b = mp \pm nq \quad \text{et} \quad a = 3mq \mp np.$$

Cum igitur numeri a et b necessario hoc modo exprimantur, siquidem numerus $aa + 3bb$ per $pp + 3qq$ fuerit divisibilis, hinc obtinebimus

$$aa + 3bb = 3mmpp + 9mmqq + 3nnqq + nnpp = (pp + 3qq)(nn + 3mm)$$

unde patet, hunc numerum, per numerum primum $P = pp + 3qq$ divisum, pro quoto dare $nn + 3mm$, hoc est numerum formae $aa + 3bb$.

15. **Coroll. 1.** Quoties ergo numerus formae $aa + 3bb$ divisorem primum habet $P = pp + 3qq$, quotus est numerus formae $nn + 3mm$. Vel, quod eodem redit, si numerus $aa + 3bb$ constet duobus factoribus, quorum alter sit primus $P = pp + 3qq$, tum etiam alter factor sive sit numerus primus, sive compositus, erit numerus formae $nn + 3mm$.

16. **Coroll. 2.** Si igitur numerus $aa + 3bb$ duobus constaret factoribus, quorum alter non in forma $nn + 3mm$ contineretur, tum alter certe non erit primus formae $pp + 3qq$.

17. **Coroll. 3.** Ex demonstratione patet, quomodo innumerabiles numeri $aa + 3bb$ exhiberi queant, qui omnes sint divisibiles per $pp + 3qq$; ejusmodi nempe numeri obtinentur capiendo

$$a = 3mq \pm np \quad \text{et} \quad b = mp \mp nq$$

neque hic amplius opus est, conditionem adjecisse, ut $pp + 3qq$ sit numerus primus; quoniam his valoribus assumtis in genere fit $aa + 3bb = (pp + 3qq)(nn + 3mm)$.

18. **Coroll. 4.** Hinc igitur vicissim intelligitur, si duo pluresve numeri quicunque formae $aa + 3bb$ in se invicem multiplicentur, productum semper fore numerum ejusdem formae. Quod enim de producto duorum valet, facile ad productum quotcunque talium numerorum extenditur.

19. **Scholion.** Etiamsi autem verum sit, productum ex duobus numeris formae $aa + 3bb$ itidem esse numerum ejusdem formae, tamen hinc per legitimam consequentiam nondum inferre licet, si numerus formae $aa + 3bb$ divisorem habeat quemcunque $pp + 3qq$, tum etiam quotum ejusdem formae esse futurum: tametsi enim et hoc verum sit, tamen peculiari indiget demonstratione mox exponenda. Ejusmodi autem conclusionem illicitam esse, vel ex hoc exemplo patebit: cum productum ex duobus numeris paribus sit numerus par, si quis inde concludere vellet, numerum parem per parem divisum quotum etiam parem esse praebiturum, is certe falleretur. Demonstrationem ergo hujus veritatis a divisore primo formae $pp + 3qq$ sum exorsus, quae conditio eatenus demonstrationem afficit, quod absque ea perperam concluderetur, cum productum $(aq + bp)(aq - bp)$ sit divisibile, alterutrum factorem divisibilem esse debere per $pp + 3qq$. Deinde vero etiam ex eo, quod p et q sint numeri inter se primi, derivavimus producti $p(mp \pm b)$, quod per q est divisibile, factorem $mp \pm b$ per q divisibilem esse debere, quae posterior conditio cum priore necessario est connexa.

20. **Propositio 5.** Si numerus $aa + 3bb$ fuerit divisibilis per productum ex duobus pluribusve numeris primis formae $pp + 3qq$, tum etiam quotus erit numerus ejusdem formae, puta $nn + 3mm$.

Demonstratio. Sint enim P, Q, R, etc. numeri primi formae $pp + 3qq$, numerusque $aa + 3bb$ divisibilis per productum PQR. Sit M quotus inde resultans, ita ut sit

$$aa + 3bb = MPQR.$$

Cum igitur sit $\frac{aa+3bb}{P} = MQR$, erit per propositionem praecedentem MQR numerus ejusdem formae. Ponatur itaque $MQR = cc + 3dd$, erit $\frac{cc+3dd}{Q} = MR$: ideoque, ob eandem rationem, hic quotus MR numerus ejusdem formae statuatur, itaque $MR = ee + 3ff$, et cum sit $\frac{ee+3ff}{R} = M$, erit pariter M numerus formae $nn + 3mm$.

21. **Coroll. 1.** Si ergo numerus $aa + 3bb$ fuerit productum ex numeris quotcunque primis P, Q, R, S, etc. formae $pp + 3qq$, et praeterea numero M, ita ut sit $aa + 3bb = MPQRS$, certo affirmare poterimus, hunc numerum M esse ejusdem formae, seu $M = nn + 3mm$.

22. **Coroll. 2.** Quodsi igitur numerus $aa + 3bb$ unum habeat factorem A, qui non sit numerus formae $nn + 3mm$, tum alter factor neque erit numerus primus formae $pp + 3qq$, neque productum ex duobus pluribusve hujusmodi numeris primis.

23. **Coroll. 3.** Eodem ergo casu si ponamus $aa + 3bb = AB$, et A non fuerit numerus formae $nn + 3mm$; tum B unum saltem factorem primum complectetur, qui non erit hujus formae. Nam si B est numerus primus, non erit formae $pp + 3qq$; sin autem non est primus, quia non ex meris numeris primis formae $pp + 3qq$ constabit, unum ad minimum factorem continebit, qui non sit ejusdem formae.

24. **Coroll. 4.** At si existente $aa + 3bb = AB$, factor A non fuerit numerus formae $nn + 3mm$, tum vel ipse erit numerus primus, in hac forma non contentus, vel saltem factorem implicabit primum, in hac forma non contentum; si enim A ex meris numeris primis formae $pp + 3qq$ esset conflatus, ipse foret numerus ejusdem formae.

25. **Coroll. 5.** Hinc sequitur, si numerus $aa + 3bb$ unum habeat factorem primum in forma $pp + 3qq$ non contentum, tum eum insuper certo adhuc alium factorem involvere, qui aeque non in hac forma $pp + 3qq$ contineatur.

26. **Coroll. 6.** Ita jam ante vidimus, si numerus $aa + 3bb$ sit par, seu factorem habeat 2 qui numerus non est formae $pp + 3qq$, tum eum insuper eundem factorem 2 complecti, seu non solum per 2, sed etiam per 4, esse divisibilem.

27. **Scholion.** Exhiberi quidem possunt numeri formae $aa + 3bb$, qui per numerum quemcunque N sint divisibiles, etiamsi N non sit numerus formae $pp + 3qq$; dum scilicet pro a et b multipla quaecunque hujus numeri N accipiuntur: ita posito $a = mN$, et $b = nN$, numerus

$$aa + 3bb = NN(mm + 3nn),$$

non solum per N, sed adeo per ejus quadratum NN, fit divisibilis: hocque ergo casu utique duo adsunt factores N et N, quorum neuter in forma $pp + 3qq$ continetur, uti § 25 ostendimus. Verum si a et b sint numeri inter se primi, hic casus locum habere nequit, ex quo merito dubitamus, num numerus inde formatus $aa + 3bb$ praeter binarium ullum admittat divisorem, qui non sit formae $pp + 3qq$? De binario quidem hoc negari nequit, cum quoties a et b fuerint numeri impares ambo, divisio per 2 succedat, at vero tum insuper binarius inest, qui cum illo conjunctus

praebet factorem 4, quasi simplicem spectandum. Diligentius igitur examinandum restat, utrum, dum a et b sunt primi inter se, numerus $aa + 3bb$ habeat ullum divisorem primum, qui non in forma $pp + 3qq$ contineatur, nec ne? quod quidem esse negandum mox rigide sum demonstraturus; in quo negotio autem probe est cavendum, ne casus binarii, quem excipi oportet, in demonstratione quicquam turbet.

28. **Propositio 6.** Si daretur numerus primus A, in forma $pp + 3qq$ non contentus, qui esset divisor cujuspiam numeri $aa + 3bb$, numeris a et b existentibus inter se primis, tum exhiberi posset alius numerus primus praeter binarium, minor B, in forma $pp + 3qq$ pariter non contentus, qui etiam futurus esset divisor cujuspiam numeri formae $aa + 3bb$, in quo numeri a et b itidem forent inter se primi.

Demonstratio. Quia a et b sunt numeri primi inter se, et $aa + 3bb$ per A divisibilis ponitur, erunt ii quoque primi ad A. Si illi numeri essent majores, quam A, statui posset

$$a = mA \pm c \quad \text{et} \quad b = nA \pm d,$$

ut numeri c et d, qui pariter tum inter se, quam ad A, futuri essent primi, forent semissi ipsius A minores, scilicet $c < \frac{1}{2}A$ et $d < \frac{1}{2}A$, quia A, utpote primus, est impar; casum enim quo $A = 2$ hinc excipimus. Prodiret autem hac positione

$$aa + 3bb = mmAA \pm 2mAc + cc + 3nnAA \pm 6nAd + 3dd$$

hincque obtineretur numerus $cc + 3dd$ minor quam AA, qui esset per A divisibilis, et quotus foret minor, quam A. Cum igitur A sit per hypothesin numerus in forma $pp + 3qq$ non contentus, vel ipse quotus, si fuerit primus, non erit numerus formae $pp + 3qq$, vel, si sit compositus, factorem habebit primum in hac forma non contentum. Sit B vel ipse quotus vel iste ejus factor, eritque certe $B < A$, ex quo daretur numerus primus B minor quam A, in forma $pp + 3qq$ non contentus, qui esset divisor numeri $cc + 3dd$, existentibus numeris c et d inter se primis.

Dico autem hunc numerum primum B a binario fore diversum. Vel enim quotus $\frac{cc + 3dd}{A}$ foret impar, vel par: et casu priori binarius in eo non contineretur, sicque numerus B non esset 2. Casu autem posteriori quotus binarium quidem, atque adeo quaternarium involveret; unde cum 4 sit numerus formae $pp + 3qq$, necesse esset, ut ille quotus alium insuper factorem primum in forma $pp + 3qq$ non contentum implicaret. Vel si $cc + 3dd$ esset per 4 divisibilis, quod eveniret, si uterque numerus c et d esset impar, ejus quadrans $\frac{1}{4}(cc + 3dd)$ ad formam $ee + 3ff$ reduci posset, quae cum per A etiam nunc foret divisibilis, multo magis quotus $\frac{ee + 3ff}{A}$ implicaret factorem primum imparem in forma $pp + 3qq$ non contentum.

29. **Propositio 7.** Omnes numeri hujus formae $aa + 3bb$, siquidem a et b sint numeri primi inter se, praeter binarium nullos admittunt divisores primos, nisi qui ipsi in forma $pp + 3qq$ contineantur.

Demonstratio. Si enim numerus quispiam formae $aa + 3bb$ haberet factorem primum quantumvis magnum A, qui in forma $pp + 3qq$ non contineretur, ex eo inveniri posset alius numerus primus B, minor quam A, nec in forma $pp + 3qq$ contentus, qui pariter esset divisor cujuspiam numeri formae $aa + 3bb$, existentibus a et b numeris inter se primis; atque ex hoc numero B

simili modo alii C, D, E continuo minores ejusdem indolis inveniri possent, haecque diminutio nunquam terminaretur, neque etiam unquam ad binarium perveniretur. Cum igitur exhibitio numerorum integrorum continuo minorum involvat contradictionem: sequitur praeter binarium nullum dari numerum primum in forma $pp+3qq$ non contentum, per quem ullus numerus formae $aa+3bb$ dividi queat, existentibus a et b numeris inter se primis.

30. **Coroll. 1.** Omnes ergo divisores primi, qui conveniunt numeris formae $aa+3bb$, siquidem a et b sint numeri inter se primi, ipsi in eadem forma $pp+3qq$ continentur; dummodo hinc binarius excludatur.

31. **Coroll. 2.** Si igitur numeri primi in duas classes distribuantur, quarum prior contineat eos, qui sunt formae $pp+3qq$; posterior vero eos, qui ad hanc formam reduci nequeunt: omnes numeri hujus posterioris classis ex serie divisorum numerorum formae $aa+3bb$ excluduntur.

32. **Coroll. 3.** Nisi ergo numerus $aa+3bb$, existentibus a et b numeris inter se primis, ipse sit primus, erit is productum ex meris numeris primis formae $pp+3qq$; dummodo quaternarius etiam inter hos numeros referatur.

33. **Scholion.** Quod productum ex duobus pluribusve numeris formae $pp+3qq$ iterum in forma $aa+3bb$ contineatur, supra ostendimus; indeque ergo patebat, si P, Q, R, S, etc. denotent numeros primos in forma $pp+3qq$ contentos, productum ex quotcunque hujusmodi numeris P, Q, R, S, etc. semper ad formam $aa+3bb$ revocari posse. Nunc autem hujus propositionis inversam demonstravimus, qua patet, numeros formae $aa+3bb$ nullos alios factores admittere, nisi qui ipsi sint numeri formae $pp+3qq$. Hic quidem assumsimus, numeros a et b esse primos inter se: sin autem non essent primi, sed maximum haberent divisorem communem m, ut sit $a=mc$ et $b=md$, tum numerus $aa+3bb=mm(cc+3dd)$ primum habebit factorem quadratum mm, cujus radix potest esse numerus quicunque, praeterea vero alios non involvet factores primos, nisi qui ipsi sint formae $pp+3qq$.

34. **Propositio 8.** Omnis numerus primus formae $pp+3qq$, si per 6 dividatur, relinquit unitatem, seu in forma numerorum $6n+1$ continetur; excepto ternario, qui etiam in forma $pp+3qq$ continetur.

Demonstratio. Cum $pp+3qq$ sit numerus primus, quadratum pp per ternarium non est divisibile, sed per 3 divisum relinquit 1; quia ergo $3qq$ divisionem per 3 admittit, summa $pp+3qq$ per 3 divisa residuum dabit $=1$; eritque propterea numerus formae $3m+1$. Cum autem $pp+3qq$ simul sit numerus impar per hypothesin, necesse est, ut m sit numerus par; unde, posito $m=2n$, formula $6n+1$ omnes complectetur numeros primos in forma $pp+3qq$ contentos; excepto scilicet ternario ipso, cujus singularis est ratio.

35. **Coroll. 1.** Quia omnes numeri primi, exceptis 2 et 3, vel in hac formula $6n+1$, vel in hac $6n-1$. continentur, evidens est, nullos numeros primos posterioris formae $6n-1$, in forma $pp+3qq$ contineri.

36. **Coroll. 2.** Hinc omnes numeri primi formae $6n-1$ qui sunt:

5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, etc.

ex divisoribus numerorum formae $aa+3bb$ sunt excludendi, seu nullus numerus hujus formae

$aa + 3bb$, dum quidem sint a et b numeri primi inter se, exhiberi potest, qui per ullum numerum primum formae $6n - 1$ sit divisibilis.

37. **Scholion.** Utrum autem omnes numeri primi alterius formae $6n + 1$, qui sunt:

7, 13, 19, 31, 37, 43, 61, 67, 73, 79. 97, etc.

sint divisores numerorum formae $aa + 3bb$; seu, quod eodem redit, an omnes in forma $pp + 3qq$ contineantur? ex allatis nondum affirmare licet. Inde enim tantum constat, omnes numeros primos formae $pp + 3qq$ simul in forma $6n + 1$ contineri, et propositio inversa peculiari indiget demonstratione, quae ita concinnari debet, ut proposito numero primo formae $6n + 1$ quocunque, ostendatur, semper quempiam numerum formae $aa + 3bb$, in quo a et b sint numeri primi inter se, exhiberi posse, qui per illum numerum $6n + 1$ sit divisibilis: in quo negotio loco formae $aa + 3bb$ etiam haec $ff \pm fg + gg$ illi aequivalens accipi potest. Si enim numerorum f et g alteruter, puta g, fuerit par, erit

$$ff \pm fg + gg = (f \pm \tfrac{1}{2}g)^2 + 3(\tfrac{1}{2}g)^2$$

sin autem uterque sit impar, erit tam $f + g$, quam $f - g$, numerus par, et

$$ff \pm fg + gg = \frac{(f \pm g)^2}{2} + 3\frac{(f \pm g)^2}{2}.$$

Quodsi ergo exhiberi queat numerus $ff \pm fg + gg$ per numerum primum $6n + 1$ divisibilis, ita ut f et g sint primi inter se, simul constabit, numerum $6n + 1$ esse numerum in forma $pp + 3qq$ contentum; id quod in sequente propositione demonstrabimus.

38. **Propositio 9.** Omnis numerus primus formae $6n + 1$ simul in hac forma $pp + 3qq$ continetur.

Demonstratio. Jam dudum demonstravi, si $6n + 1$ fuerit numerus primus, per eum divisibiles esse omnes numeros in hac forma $a^{6n} - b^{6n}$ contentos, dummodo neuter numerorum a et b seorsim per $6n + 1$ sit divisibilis (*). Cum igitur in factores resolvendo sit

$$a^{6n} - b^{6n} = (a^{2n} - b^{2n})(a^{4n} + a^{2n}b^{2n} + b^{4n})$$

alteruter horum factorum per $6n + 1$ sit divisibilis necesse est. Quodsi ergo dentur casus, quibus factor $a^{2n} - b^{2n}$ non sit divisibilis per $6n + 1$, ut tamen neque a, neque b per eum sit divisibilis, iis casibus certe alter factor $a^{4n} + a^{2n}b^{2n} + b^{4n}$, hoc est numerus formae $ff + fg + gg$, per $6n + 1$ erit divisibilis, ideoque numerus primus $6n + 1$ foret in forma $pp + 3qq$ contentus. Demonstrari igitur debet, dari casus, quibus forma $a^{2n} - b^{2n}$ non sit divisibilis per $6n + 1$. Ad hoc efficiendum sumo $b = 1$, et ostendam, fieri non posse, ut omnes isti numeri:

$$2^{2n} - 1,\ 3^{2n} - 1,\ 4^{2n} - 1,\ 5^{2n} - 1,\ \ldots\ (6n)^{2n} - 1,$$

sint per $6n + 1$ divisibiles, ubi quidem pro a omnes numeros ipso $6n + 1$ minores, ideoque primos ad eum, assumi pono. Nam si omnes hi numeri per $6n + 1$ essent divisibiles, eorum etiam differentiae, cum primae, tum secundae, et sequentes omnes, per $6n + 1$ essent divisibiles, ideoque etiam differentiae ordinis $2n$, quae sunt omnes constantes, et hoc modo exprimuntur:

$$2^{2n} - \frac{2n}{1}\cdot 3^{2n} + \frac{2n(2n-1)}{1.2}4^{2n} - \frac{2n(2n-1)(2n-2)}{1.2.3}5^{2n}\ \ldots\ (2+2n)^{2n}$$

(*) Vide pag. 52, theorema 4.

ubi, cum sit $2n + 2 < 6n$, nullae potestates numerorum per $6n + 1$ divisibilium ingrediuntur. Aliunde autem constat, differentiam ordinis $2n$ esse $= 1.2.3.4 \ldots 2n$, quae, cum certe non sit per $6n + 1$ divisibilis, manifesto indicat, reperiri adeo inter hos numeros:

$$2^{2n} - 1,\ 3^{2n} - 1,\ 4^{2n} - 1, \ldots (2 + 2n)^{2n} - 1$$

unum, vel etiam plures, qui non sint per $6n + 1$ divisibiles. Dum autem unicus detur hujusmodi numerus $a^{2n} - 1$ per $6n + 1$ non divisibilis, per eum erit divisibilis $a^{4n} + a^{2n} + 1$, hoc est numerus formae $ff + fg + gg$, in quo neque f, neque g, sit per $6n + 1$ divisibilis. Consequenter numerus primus $6n + 1$ est formae $pp + 3qq$.

39. **Scholion.** Omnia ergo, quae cum in demonstratione theorematis, non dari duos cubos, quorum summa sit cubus, tum in solutione problematis de inveniendis tribus cubis, quorum summa sit cubus, assumseram, jam plane rigide sunt demonstrata. Assumseram autem primo, numeros formae $aa + 3bb$, seu $ff \pm fg + gg$, nullos admittere divisores primos, nisi qui ipsi sint ejusdem formae, deinde omnes numeros primos istius formae simul in formula $6n + 1$ contineri, ac vicissim omnes numeros primos in formula $6n + 1$ contentos, simul esse numeros formae $pp + 3qq$. Quare nunc, tam illa demonstratio, quam solutio, pro perfectis sunt habendae. Interim tamen fateri cogor, in hac de natura numerorum theoria plurima etiamnum desiderari, atque Fermatii demonstrationes deperditas sine dubio multo profundiores speculationes in se esse complexas. Eo enim modo, quo usus sum ad demonstrandum, summam duorum cuborum nunquam posse esse cubum, non perspicio, quomodo demonstratio ad potestates altiores extendi possit, cum tamen Fermatius demonstrationem habuerit, neque summam $a^n + b^n$, neque differentiam $a^n - b^n$, nunquam esse potestatem similis exponentis c^n, quando exponens n fuerit binario major. Demonstrandum ergo esset, hanc aequationem $a^n \pm b^n = c^n$ in rationalibus nunquam locum habere posse, statim atque exponens n binarium superet, nisi unus numerorum a, b, c evanescat. Deinde etsi demonstravi, numeros primos omnes formae $6n + 1$ esse in formula $pp + 3qq$ contentos, tamen simili modo demonstrare non licet, numeros primos formae $8n + 3$ semper in forma $pp + 2qq$ contineri, quod tamen aeque est certum, et a Fermatio demonstratum. Successit mihi quidem demonstratio, quod numeri primi formae $4n + 1$ sint omnes duorum quadratorum summae, similique modo demonstrare possum, omnes numeros primos formae $8n + 1$ simul in forma $pp + 2qq$ contineri: verum plurima ejusdem generis theoremata proferri possunt aeque vera, veluti quod omnes numeri primi vel hujus formae $20n + 1$, vel $20n + 9$, simul in formula $pp + 5qq$ contineantur, et hujusmodi plura alia, quae tamen nondum video, quomodo demonstrari queant. Ex quo theoria numerorum nobis adhuc maximam partem abscondita est censenda.

XXII.

De resolutione formularum quadraticarum indeterminatarum per numeros integros.

(N. Comment. IX. 1762—63. p. 3. Exhib. 1759 Oct. 15.)

1. **Problema 1.** Proposita formula irrationali $\sqrt{(\alpha xx + \beta x + \gamma)}$ invenire numeros pro x substituendos, qui eam rationalem reddant.

Solutio. Ante omnia notandum est, hanc investigationem frustra suscipi, nisi unus saltem casus constet, quo ea fiat rationalis. Ponamus ergo hoc evenire casu $x = a$, eoque esse:

$$\sqrt{(\alpha aa + \beta a + \gamma)} = b$$

ita ut b sit numerus rationalis. Hujusmodi autem casus, unico cognito, innumerabiles alios ex eo derivare licet. Ponatur in hunc finem

$$x = a + mz \quad \text{et} \quad \sqrt{(\alpha xx + \beta x + \gamma)} = b + nz$$

et hac aequatione quadrata fit:

$$\left.\begin{array}{l} + \alpha aa + 2\alpha maz + \alpha mmzz \\ + \beta a + \beta mz \\ + \gamma. \end{array}\right\} = bb + 2nbz + nnzz$$

Cum jam per hypothesin sit $bb = \alpha aa + \beta a + \gamma$, reliqua aequatio per z divisa dabit:

$$2\alpha ma + \beta m + \alpha mmz = 2nb + nnz$$

ex qua elicitur:

$$z = \frac{2\alpha ma - 2nb + \beta m}{nn - \alpha mm}.$$

Quo valore substituto concludimus:

$$\text{si ponatur } x = \frac{(nn + \alpha mm)a - 2mnb + \beta mm}{nn - \alpha mm}$$

$$\text{fore } \sqrt{(\alpha xx + \beta x + \gamma)} = \frac{2\alpha mna - (nn + \alpha mm)b + \beta mn}{nn - \alpha mm}.$$

Quicunque ergo numeri pro m et n accipiantur, ex casu cognito: $\sqrt{\alpha aa + \beta a + \gamma)} = b$, infinitis aliis modis formula $\sqrt{(\alpha xx + \beta x + \gamma)}$ rationalis effici potest, et quia numerum b tam negative, quam affirmative assumere licet, exploratis numeris a et b, ac pro lubitu assumtis numeris m et n, capiatur

$$x = \frac{(nn + \alpha mm)a \pm 2mnb + \beta mm}{nn - \alpha mm}$$

eritque:

$$\sqrt{\alpha xx + \beta x + \gamma)} = \frac{2\alpha mna \pm (nn + \alpha mm)b + \beta mn}{nn - \alpha mm}.$$

2. **Scholion.** Ad hoc ergo problema solvendum necesse est, ut aliunde unus saltem casus sit cognitus, quo formula proposita fiat rationalis. Neque vero, pro hujusmodi casu explorando ulla certa regula praescribi potest, cum etiam dentur ejusmodi formulae, quas nullo plane casu rationales fieri posse demonstratum est. Si enim verbi gratia haec formula $\sqrt{(3xx+2)}$ proponeretur, certum est, nullum numerum rationalem pro x inveniri posse, quo ea fieret rationalis. Quanquam autem satis noti sunt casus, quibus formula $\alpha xx+\beta x+\gamma$ talis reductionis est capax, quippe quod evenit, quoties in hac formula generali $(px+q)^2+(rx+s)(tx+u)$ continetur: tamen hic non curo, unde casus ille, quem cognitum assumo, sit haustus, sive certa quadam ratione, sive divinatione innotuerit. Verum cum cognito uno casu, inventio infinitorum aliorum nulla laboret difficultate, hic potissimum ad solutiones, quae numeris integris absolvuntur, respicio. Cum enim valores pro x inventi per fractionem exprimantur, nova jam oritur quaestio, quomodo numeros m et n assumi oporteat, ut inde numeri integri pro x obtineantur.

3. **Problema 2.** Si α, β, γ sint numeri integri dati, invenire numeros integros pro x sumendos, qui formulam $\alpha xx+\beta x+\gamma$ quadratam reddant.

Solutio. Iterum assumo unum numerum integrum a constare, qui quaesito satisfaciat, ita ut sit: $\sqrt{(\alpha aa+\beta a+\gamma)}=b$; ac modo vidimus,

$$\text{si sumatur} \quad x=\frac{(nn+\alpha mm)a\pm 2mnb+\beta mn}{nn-\alpha mm}$$

$$\text{fore} \quad \sqrt{(\alpha xx+\beta x+\gamma)}=\frac{2\alpha mna\pm(nn+\alpha mm)b+\beta mn}{nn-\alpha mm}.$$

Superest ergo tantum, ut videamus, cujusmodi numeros pro m et n assumi oporteat, ut hae formulae integrae evadant. Quod quidem statim fieri perspicuum est, si utriusque denominator $nn-\alpha mm$ statuatur unitati aequalis. Sit igitur $nn-\alpha mm=1$, seu

$$nn=\alpha mm+1, \quad \text{ideoque} \quad n=\sqrt{(\alpha mm+1)},$$

nisi autem sit α vel numerus quadratus, vel negativus, huic formulae semper satisfieri potest; sin autem sit vel quadratus, vel negativus, ne problema quidem propositum resolvere licet. Etsi enim quandoque duo pluresve casus assignari queant, tamen infiniti non dantur, cujusmodi tamen hic evolvi convenit. Sit ergo α numerus integer positivus non quadratus, ac semper numeri m et n assignari possunt, ut fiat $n=\sqrt{(\alpha mn+1)}$, quod etsi infinitis modis fieri potest, tamen sufficit minimos solos nosse. Erit ergo

$$x=(nn+\alpha mm)a\pm 2mnb+\beta mm \quad \text{et} \quad \sqrt{(\alpha xx+\beta x+\gamma)}=2\alpha mna\pm(nn+\alpha mm)b+\beta mn,$$

sicque habetur novus casus quaestioni satisfaciens. Ex hoc vero simili modo, quo is ex a et b prodiit, novus derivabitur, hincque porro continuo alii in infinitum. Ponantur enim valores hoc modo pro x oriundi successive: a, a', a'', a''', etc. respondentes vero valores formulae $\sqrt{(\alpha xx+\beta x+\gamma)}$ sint b, b', b'', b''', etc. ac sequenti modo bini quique posteriores ex binis antecedentibus definientur:

$$\begin{aligned} a' &= (nn+\alpha mm)a \pm 2mnb + \beta mm, & b' &= 2\alpha mna \pm (nn+\alpha mm)b + \beta mn, \\ a'' &= (nn+\alpha mm)a' \pm 2mnb' + \beta mm, & b'' &= 2\alpha mna' \pm (nn+\alpha mm)b' + \beta mn, \\ a''' &= (nn+\alpha mm)a'' \pm 2mnb'' + \beta mm, & b''' &= 2\alpha mna'' \pm (nn+\alpha mm)b'' + \beta mn, \end{aligned}$$

etc.

Hac igitur ratione continuo ulterius progredi licet, sicque ex una solutione, in numeris integris cognita, innumerabiles aliae in numeris integris quoque elicientur.

4. **Coroll. 1.** Ut igitur formula $\alpha xx + \beta x + \gamma$ infinitis modis in numeris integris quadratum effici possit, necesse est, ut α neque sit numerus quadratus, neque negativus, ac praeterea, ut unus casus, quo ea fit quadratum, undecunque sit cognitus.

5. **Coroll. 2.** At si α fuerit numerus positivus non quadratus, tum primum quaerantur duo numeri m et n, ut sit $n = \sqrt{(\alpha mm + 1)}$, id quod semper fieri potest. Quibus inventis, si ponatur: $\sqrt{(\alpha xx + \beta x + \gamma)} = y$ atque jam cognitus fuerit casus quaestioni satisfaciens, qui sit $x = a$ et $y = b$, ex eo per primam operationem non solum unus, sed duo novi invenientur ob signi ambiguitatem. Erit quippe:

$$x = (nn + \alpha mm)\, a \pm 2mnb + \beta mm \quad \text{et}$$
$$y = 2\alpha mna \pm (nn + \alpha mm)\, b + \beta mn.$$

6. **Coroll. 3.** Si sumantur tantum signorum ambiguorum superiora, ut continuo ad majores numeros satisfacientes perveniamus, atque valores pro x hoc modo successive prodeuntes designentur per a, a', a'', a''', a^{IV}, etc. valores autem pro y respondentes per b, b', b'', b''', b^{IV}, etc. erit:

$$a' = (nn + \alpha mm)\, a + 2mnb + \beta mm, \quad b' = 2\alpha mna + (nn + \alpha mm)\, b + \beta mn,$$
$$a'' = (nn + \alpha mm)\, a' + 2mnb' + \beta mm, \quad b'' = 2\alpha mna' + (nn + \alpha mm)\, b' + \beta mn,$$
$$a''' = (nn + \alpha mm)\, a'' + 2mnb'' + \beta mm, \quad b''' = 2\alpha mna'' + (nn + \alpha mm)\, b'' + \beta mn,$$

etc.

7. **Coroll. 4.** Duplicem ergo hinc progressionem numerorum a, a', a'', a''', a^{IV}, etc. et b, b', b'', b''', b^{IV}, etc. adipiscimur, quarum utriusque continuatio ab utraque pendet, utraque tamen ab altera ista sejungi potest, ut termini utriusque sensim sine adminiculo alterius continuari queant; formabitur autem tum in utraque serie quilibet terminus ex binis praecedentibus.

8. **Coroll. 5.** Si enim in valore a'' pro b' ejus valor substituatur, habebitur:

$$a'' = (nn + \alpha mm)\, a' + 4\alpha mmnna + 2mn\,(nn + \alpha mm)\, b + 2\beta mmnn + \beta mm.$$

Verum ex valore ipsius a' est:

$$2mnb = a' - (nn + \alpha mm)\, a - \beta mm$$

quo valore ipsius $2mnb$ ibi substituto prodibit:

$$\begin{aligned} a'' = {} & (nn + \alpha mm)\, a' + 4\alpha mmnna \\ & + (nn + \alpha mm)\, a' - (nn + \alpha mm)^2\, a - \beta mm\,(nn + \alpha mm) \\ & + 2\beta mmnn \\ & + \beta mm. \end{aligned}$$

At ob $nn = \alpha mm + 1$, est

$$4\alpha mmnn - (nn + \alpha mm)^2 = -(nn - \alpha mm)^2 = -1 \quad \text{et}$$
$$2\beta mmnn - \beta mm\,(nn + \alpha mm) = \beta mm\,(nn - \alpha mm) = \beta mm,$$

unde fit:

$$a'' = 2\,(nn + \alpha mm)\, a' - a + 2\beta mm.$$

9. **Coroll. 6.** Cum igitur simili modo sit:

$$a''' = 2(nn + \alpha mm)a'' - a' + 2\beta mm \text{ etc.}$$

Statim atque in serie a, a', a'', a''', etc. duo primi termini habentur, primus scilicet a undecunque, et secundus ex formula

$$a' = (nn + \alpha mm)a + 2mnb + \beta mm,$$

ex his sequentes omnes per has formulas definientur:

$$a'' = 2(nn + \alpha mm)a' - a + 2\beta mm,$$
$$a''' = 2(nn + \alpha mm)a'' - a' + 2\beta mm,$$
$$a^{IV} = 2(nn + \alpha mm)a''' - a'' + 2\beta mm.$$

10. **Coroll. 7.** Pari autem modo progressio numerorum b, b', b'', b''', etc. est comparata. Primo enim ejus termino aliunde cognito, et secundo per formulam

$$b' = 2\alpha mna + (nn + \alpha mm)b + \beta mn,$$

si in b'' pro a' valor substituatur, erit:

$$b'' = 2\alpha mn(nn + \alpha mm)a + 4\alpha mmnnb + 2\alpha\beta m^3 n + (nn + \alpha mm)b' + \beta mn$$

at ex valore ipsius b' est $2\alpha mna = b' - (nn + \alpha mm)b - \beta mn$, quo substituto fit, ob $nn - \alpha mm = 1$,

$$b'' = 2(nn + \alpha mm)b' - b, \quad \text{similiterque}$$
$$b''' = 2(nn + \alpha mm)b'' - b',$$
$$b^{IV} = 2(nn + \alpha mm)b''' - b'',$$

etc.

11. **Coroll. 8.** Cum igitur utraque series ita sit comparata, ut quilibet terminus ex binis praecedentibus secundum certam legem definiatur, utraque series erit recurrens, scala relationis existente $2(nn + \alpha mm)$, -1. Hinc ergo, formata aequatione $zz = 2(nn + \alpha mm)z - 1$, ejus radices erunt:

$$z = 2nn - 1 \pm 2n\sqrt{(nn - 1)} = (n \pm m\sqrt{\alpha})^2.$$

12. **Coroll. 9.** Hinc ergo ex doctrina serierum recurrentium progressionis a, a', a'', a''', a^{IV}, etc. terminus quicunque indefinite per sequentem formulam exprimetur:

$$\left(\frac{a}{2} + \frac{\beta}{4\alpha} + \frac{b}{2\sqrt{\alpha}}\right)(n + m\sqrt{\alpha})^{2\nu} + \left(\frac{a}{2} + \frac{\beta}{4\alpha} - \frac{b}{2\sqrt{\alpha}}\right)(n - m\sqrt{\alpha})^{2\nu} - \frac{\beta}{2\alpha} = x$$

alterius vero seriei b, b', b'', b''', etc. terminus quicunque per hanc:

$$\left(\frac{b}{2} + \frac{a\sqrt{\alpha}}{2} + \frac{\beta}{4\sqrt{\alpha}}\right)(n + m\sqrt{\alpha})^{2\nu} + \left(\frac{b}{2} - \frac{a\sqrt{\alpha}}{2} - \frac{\beta}{4\sqrt{\alpha}}\right)(n - m\sqrt{\alpha})^{2\nu} = y$$

sumto pro ν numero quocunque integro.

13. **Scholion.** Si hic pro 2ν substituamus successive omnes numeros integros 0, 1, 2, 3, 4, 5, etc. utraque progressio prodibit interpolata, cujus termini medii quaesito aeque satisfacient, dummodo fuerint integri. At reperiemus, posito

$2\nu = 0$,	$x = a$,	$y = b$,
$2\nu = 1$,	$x = na + mb + \frac{\beta(n-1)}{2\alpha}$,	$y = nb + \alpha ma + \frac{\beta m}{2}$,
$2\nu = 2$,	$x = (nn + \alpha mm)a + 2mnb + \beta mm$,	$y = (nn + \alpha mm)b + 2\alpha mna + \beta mn$.

Quae utraque series est recurrens, scalam relationis habens $2n$, -1, ac pro priori quidem valorum ipsius x, si terni termini consecutivi sint P, Q, R, erit

$$R = 2nQ - P + \frac{\beta(n-1)}{\alpha};$$

at si in progressione valorum ipsius y terni termini se ordine sequentes sint P, Q et R, erit

$$R = 2nQ - P.$$

Quodsi ergo fuerit $\frac{\beta(n-1)}{2\alpha}$ numerus integer, omnes hi termini problema aeque resolvent, sicque duplo plures obtinebimus solutiones, quam methodus adhibita suppeditaverat. Quod autem plures locum habere possint solutiones, quam invenimus, inde facile colligitur, quod praeter necessitatem primam erutarum formularum $nn - \alpha mm$ unitati aequalem posuimus, cum tamen sine dubio saepe etiam numerator per denominatorem dividi possit, etiamsi hic unitate sit major. Quemadmodum igitur omnes plane solutiones in numeris integris inveniri queant, sequenti problemate accuratius examinemus.

14. **Problema 3.** Si α sit numerus integer positivus non quadratus, dato uno numero integro a, qui pro x positus reddat formulam $\alpha xx + \beta x + \gamma$ quadratam, invenire infinitos alios numeros integros, qui pro x sumti idem sint praestituri.

Solutio. Ponatur in genere $\sqrt{(\alpha xx + \beta x + \gamma)} = y$, casu autem cognito, quo $x = a$, esse $\sqrt{(\alpha aa + \beta a + \gamma)} = b$, atque hinc in genere, fractionibus non exclusis, fore vidimus:

$$x = \frac{(nn + \alpha mm)a + 2mnb + \beta mm}{nn - \alpha mm},$$

$$y = \frac{(nn + \alpha mm)b + 2\alpha mna + \beta mn}{nn - \alpha mm}.$$

Jam quidem, ut hi numeri fiant integri, non absolute necesse est, ut denominator $nn - \alpha mm$ ad unitatem revocetur, verum sufficit, ut fractiones $\frac{nn + \alpha mm}{nn - \alpha mm}$ et $\frac{2mn}{nn - \alpha mm}$ in numeros integros abeant. Ponamus ergo esse

$$\frac{nn + \alpha mm}{nn - \alpha mm} = p, \quad \text{et} \quad \frac{2mn}{nn - \alpha mm} = q,$$

unde fit $p - 1 = \frac{2\alpha mm}{nn - \alpha mm}$; ideoque

$$\frac{\beta mm}{nn - \alpha mm} = \frac{\beta}{2\alpha}(p-1) \quad \text{et} \quad \frac{\beta mn}{nn - \alpha mm} = \tfrac{1}{2}\beta q.$$

Deinde autem ex formulis assumtis fiet

$$pp - \alpha qq = \frac{(nn + \alpha mm)^2 - 4\alpha mmnn}{(nn - \alpha mm)^2} = 1$$

ita ut sit $$pp = \alpha qq + 1 \quad \text{et} \quad p = \sqrt{(\alpha qq + 1)}.$$

Iterum igitur ut ante ex numero α binos numeros p et q assignari oportet, ut sit $p = \sqrt{(\alpha qq + 1)}$, quibus inventis habebitur:

$$x = pa + qb + \frac{\beta}{2\alpha}(p-1) \quad \text{et} \quad y = pb + \alpha qa + \tfrac{1}{2}\beta q.$$

Dummodo ergo fuerit $\frac{\beta}{2\alpha}(p-1)$ numerus integer, hi valores satisfaciunt. Quia autem numeros p et q tam negative, quam positive sumere licet, hae formulae insuper tres alias solutiones suppeditant:

$$x = pa - qb + \frac{\beta}{2a}(p-1) \quad \text{et} \quad y = pb - \alpha qa - \tfrac{1}{2}\beta q,$$
$$x = -pa + qb - \frac{\beta}{2a}(p+1) \quad \text{et} \quad y = -pb + \alpha qa + \tfrac{1}{2}\beta q,$$
$$x = -pa - qb - \frac{\beta}{2a}(p+1) \quad \text{et} \quad y = -pb - \alpha qa - \tfrac{1}{2}\beta q.$$

Quod si porro horum bini quicunque pro a et b assumantur, ex quolibet quatuor novae solutiones orientur. Hinc tamen non 16, sed tantum sex diversae oriuntur, inter quas adeo prima cognita $x = a$ et $y = b$, et quae huic est affinis $x = -a - \frac{\beta}{\alpha}$, et $y = b$ continentur; reliquae vero quatuor sunt

$$x = (pp + \alpha qq)\,a \pm 2pqb + \beta qq, \quad y = (pp + \alpha qq)\,b \pm 2\alpha pqa \pm \beta pq,$$
$$x = -(pp + \alpha qq)\,a \pm 2pqb - \frac{\beta}{\alpha}pp, \quad y = (pp + \alpha qq)\,b \mp 2\alpha pqa \mp \beta pq,$$

ex quibus deinceps novae aliae in infinitum inveniri possunt.

15. **Coroll. 1.** Quodsi ergo fuerit vel $\beta = 0$, vel ejusmodi numerus, ut $\beta(p-1)$, vel etiam $\beta(p+1)$ per 2α divisibile existat, tum hoc modo plures solutiones in integris obtinentur, quam modo ante exposito.

16. **Coroll. 2.** In genere autem observandum est, si satisfecerit casus quicunque $x = v$, tum etiam satisfacturum esse casum $x = -v - \frac{\beta}{\alpha}$, ex utroque enim y eundem valorem nanciscitur. Quare cum hi casus ex illis tam facile eliciantur, his omissis investigatio solutionum convenientium ad dimidium reducitur.

17. **Coroll. 3.** Rejectis ergo casibus $x = -v - \frac{\beta}{\alpha}$, quippe qui sponte se produnt inventis casibus $x = v$, ex casu $x = a$ et $y = b$ statim bini reperiuntur:

$$x = pa \pm qb + \frac{\beta}{2\alpha}(p-1), \quad y = \alpha qa \pm pb + \tfrac{1}{2}\beta q$$

hincque porro per operationem secundam bini:

$$x = (pp + \alpha qq)\,a \pm 2pqb + \beta qq; \quad y = 2\alpha pqa \pm (pp + \alpha qq)\,b + \beta pq,$$

quae duplicitas ex signo ambiguo numeri b nascitur.

18. **Coroll. 4.** Si haec cum §§ 12 et 13 conferantur, patebit omnes has formulas in sequentibus expressionibus generalibus contineri, siquidem pro μ successive omnes numeri integri substituantur.

$$\text{I}\begin{cases} x = \frac{1}{4\alpha}(2\alpha a + \beta + 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^{\mu} + \frac{1}{4\alpha}(2\alpha a + \beta - 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^{\mu} - \frac{\beta}{2\alpha} \\ y = \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta + 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^{\mu} - \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta - 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^{\mu} \end{cases}$$

et

$$\text{II}\begin{cases} x = \frac{1}{4\alpha}(2\alpha a + \beta - 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^{\mu} + \frac{1}{4\alpha}(2\alpha a + \beta + 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^{\mu} - \frac{\beta}{2\alpha} \\ y = \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta - 2b\sqrt{\alpha})(p + q\sqrt{\alpha})^{\mu} - \frac{1}{4\sqrt{\alpha}}(2\alpha a + \beta + 2b\sqrt{\alpha})(p - q\sqrt{\alpha})^{\mu} \end{cases}$$

19. **Coroll. 5.** Hinc igitur duplices series pro valoribus numerorum x et y reperiuntur, quae eandem progressionis legem tenebunt. Si enim ponamus:

$$x = a,\ a',\ a'',\ a''',\ a^{IV},\ a^{V},\ \text{etc. } P,\ Q,\ R,$$
$$y = b,\ b',\ b'',\ b''',\ b^{IV},\ b^{V},\ \text{etc. } S,\ T,\ V,$$

erit pro altera: $a' = pa + qb + \frac{\beta}{2\alpha}(p-1)$ et $b' = \alpha qa + pb + \frac{1}{2}\beta q$

et pro altera: $a' = pa - qb + \frac{\beta}{2\alpha}(p-1)$ et $b' = \alpha qa - pb + \frac{1}{2}\beta q$

pro utraque vero haec communis progressionis lex valebit, ut sit:

$$R = 2pQ - P + \frac{\beta}{\alpha}(p-1) \quad \text{et} \quad V = 2pT - S.$$

20. **Coroll. 6.** Cum sit $pp - \alpha qq = 1$, erit

$$(p + q\sqrt{\alpha})^{\mu} = (p - q\sqrt{\alpha})^{-\mu} \quad \text{et} \quad (p - q\sqrt{\alpha})^{\mu} = (p + q\sqrt{\alpha})^{-\mu},$$

hincque, si alterae series retrorsum continuentur, prodibunt alterae. Sufficit ergo pro altero casu has series instruxisse, quae tam antrorsum, quam retrorsum continuatae omnes solutiones, ex ambiguitate numeri b oriundas, in se continebunt.

21. **Schollon.** Si ergo fuerit $\beta = 0$, ut habeatur haec formula: $\sqrt{(\alpha xx + \gamma)} = y$, rationalis reddenda, casusque constet, quo sit $\sqrt{(\alpha aa + \gamma)} = b$, sumtis numeris p et q ita, ut sit $p = \sqrt{(\alpha qq + 1)}$ innumerabiles alii valores satisfacientes continebuntur in his seriebus:

$$x = a,\ a',\ a'',\ a''',\ a^{IV},\ \ldots\ P,\ Q,\ R,$$
$$y = b,\ b',\ b'',\ b''',\ b^{IV},\ \ldots\ S,\ T,\ V,$$

ubi secundi termini ita debent accipi, ut sit

$$a' = pa + qb, \quad b' = \alpha qa + pb$$

deinde utraque series est recurrens, scala relationis existente $2p,\ -1$. Erit scilicet

$$a'' = 2pa' - a, \quad \text{et in genere } R = 2pQ - P,$$
$$b'' = 2pb' - b, \quad \ldots\ldots\ldots \quad V = 2pT - S,$$

ambae vero series etiam retrorsum continuari debent, sicque duplo plures prodibunt solutiones, nisi sit vel $a = 0$, vel $b = 0$. Neque autem hic in censum veniunt solutiones negativae, quibus si satisfecerit $x = v$, etiam satisfacit $x = -v$. Omnes porro istae solutiones continentur in his formulis generalibus:

$$x = \frac{1}{2\sqrt{\alpha}}(a\sqrt{\alpha} + b)(p + q\sqrt{\alpha})^{\mu} + \frac{1}{2\sqrt{\alpha}}(a\sqrt{\alpha} - b)(p - q\sqrt{\alpha})^{\mu},$$
$$y = \frac{1}{2}(a\sqrt{\alpha} + b)(p + q\sqrt{\alpha})^{\mu} - \frac{1}{2}(a\sqrt{\alpha} - b)(p - q\sqrt{\alpha})^{\mu}.$$

Pro variis igitur numeris, qui coefficientem α constituunt, sequentia exempla evolvamus, et quidem generalius, ut etiam coefficientis β ratio habeatur, pro casibus scilicet, quibus forte $\frac{\beta}{2\alpha}(p-1)$ fuerit numerus integer.

22. **Exempl. 1.** *Proposita formula* $\sqrt{(2xx + \beta x + \gamma)} = y$, *invenire infinitos valores integros ipsius* x, *quibus haec formula rationalis evadit, siquidem una solutio constet.*

Sit solutio cognita $x=a$ et $y=b$, et ob $\alpha=2$, habebimus $p=\sqrt{(2qq+1)}$, ideoque $q=2$ et $p=3$. Hinc secundi valores erunt:

$$a'=3a\pm 2b+\frac{\beta}{2},\quad b'=4a\pm 3b+\beta.$$

Cum igitur in § 19 sit $R=6Q-P+\beta$ et $V=6T-S$, habebimus sequentes series valorum satisfacientium et quidem integrorum, si β fuerit numerus par:

Valores ipsius x	Valores ipsius y
a	$\pm b$
$3a\pm 2b+\frac{\beta}{2}$,	$4a\pm 3b+\beta$,
$17a\pm 12b+4\beta$,	$24a\pm 17b+6\beta$,
$99a\pm 70b+\frac{49}{2}\beta$,	$140a\pm 99b+35\beta$,
$577a\pm 408b+144\beta$,	$816a\pm 577b+204\beta$,
$3363a\pm 2378b+\frac{1681}{2}\beta$,	$4756a\pm 3363b+1189\beta$,
etc.	etc.

Tum vero cum y eosdem retineat valores, si pro x scribatur $-x-\frac{\beta}{2}$, etiam hae solutiones locum habebunt:

Valores ipsius x	Valores ipsius y
$-a-\frac{1}{2}\beta$,	$\pm b$
$-3a\mp 2b-\beta$,	$4a\pm 3b+\beta$,
$-17a\mp 12b-\frac{9}{2}\beta$,	$24a\pm 17b+6\beta$,
$-99a\mp 706b-25\beta$,	$140a\pm 99b+35\beta$,
$-577a\mp 408b-\frac{289}{2}\beta$,	$816a\pm 577b+204\beta$,
$-3363a\mp 2378b-841\beta$,	$4756a\pm 3363b+1189\beta$,
etc.	etc.

Etiamsi ergo β non fuerit numerus par, tamen in utroque ordine semissis valorum ipsius x praebuerit numeros integros.

23. **Exempl. 2.** *Proposita formula* $\sqrt{(3xx+\beta x+\gamma)}=y$, *invenire infinitos valores integros ipsius* x, *quibus haec formula rationalis evadit, siquidem unus casus constet.*

Praebeat casus cognitus $x=a$ et $y=b$, tum vero ob $\alpha=3$ capiatur $p=\sqrt{(3qq+1)}$, eritque $q=1$ et $p=2$. Hinc pro secundo casu habebimus:

$$a'=2a\pm b+\frac{\beta}{6},\quad b'=3a\pm 2b+\frac{\beta}{2},$$

ex quibus formentur binae series recurrentes, secundum has scalas relationis:

$$R=4Q-P+\frac{\beta}{3},\quad V=4T-S,$$

unde obtinentur:

Valores ipsius x	Valores ipsius y
a	$\pm b$,
$2a \pm b + \frac{1}{6}\beta$,	$3a \pm 2b + \frac{1}{2}\beta$,
$7a \pm b + \beta$,	$12a \pm 7b + 2\beta$,
$26a \pm 15b + \frac{25}{6}\beta$,	$45a \pm 26b + \frac{15}{2}\beta$,
$97a \pm 56b + 16\beta$,	$168a \pm 97b + 28\beta$,
$362a \pm 209b + \frac{361}{6}\beta$,	$627a \pm 362b + \frac{209}{2}\beta$,
$1351a \pm 780b + 225\beta$,	$2340a \pm 1351b + 390\beta$,
etc.	etc.

Praeterea vero scribendo $-x-\frac{\beta}{3}$ pro x, prodibunt

valores ipsius x	valores ipsius y
$-a-\frac{1}{3}\beta$,	$\pm b$,
$-2a \mp b - \frac{1}{2}\beta$,	$3a \pm 2b + \frac{1}{2}\beta$,
$-7a \mp 4b - \frac{4}{3}\beta$,	$12a \pm 7b + 2\beta$
$-26a \mp 15b - \frac{9}{2}\beta$,	$45a \pm 26b + \frac{15}{2}\beta$,
$-97a \mp 56b - \frac{49}{3}\beta$,	$168a \pm 97b + 28\beta$,
$-362a \mp 209b - \frac{121}{2}\beta$,	$627a \pm 362b + \frac{209}{2}\beta$,
$-1351a \mp 780b - \frac{676}{3}\beta$,	$2340a \pm 1351b + 390\beta$,
etc.	etc.

Prout ergo numerus β divisibilis fuerit per 2, vel 3, vel utrumque, hinc eo plures solutiones in integris eliciuntur.

24. **Exempl. 3.** *Proposita formula* $\sqrt{(5xx+\beta x+\gamma)}=y$, *invenire infinitos valores integros ipsius* x, *quibus haec formula rationalis evadat, siquidem unus casus fuerit cognitus.*

Pro casu cognito sit $x=a$ et $y=b$, et ob $\alpha=5$, quaerantur numeri p et q, ut sit $p=\sqrt{(5qq+1)}$. Fiet ergo $q=4$ et $p=9$; et hinc secunda solutio prodibit:

$$a'=9a\pm 4b+\frac{4}{5}\beta,\quad b'=20a\pm 9b+2\beta.$$

Cum ergo sit $a''=18a'-a+\frac{8}{5}\beta$ et $b''=18b'-b$, sequentes solutionos habebuntur:

Valores ipsius x	Valores ipsius y
a	$\pm b$
$9a \pm 4b + \frac{4}{5}\beta$,	$20a \pm 9b + 2\beta$,
$161a \pm 72b + 16\beta$,	$360a \pm 161b + 36\beta$,
$2889a \pm 1292b + \frac{1444}{5}\beta$,	$6460a \pm 2839b + 646\beta$,
etc.	etc.

ubi pro quolibet valore ipsius x etiam poni potest $-x-\frac{\beta}{5}$.

25. **Scholion 1.** Cum hoc modo ex una solutione in integris cognita, infinitae aliae solutiones etiam in integris eliciantur, quaestio nascitur, an hoc modo omnes plane solutiones integrae obtineantur, nec ne? Ac in exemplis quidem primo et secundo nullum erit dubium, quin hac methodo omnes solutiones integrae obtineantur. Verum in exemplo tertio utique dantur casus, quibus multo plures solutiones in integris exhiberi possunt, quam quidem hac methodo reperiuntur. Veluti si proposita fuerit formula $\sqrt{(5xx+4)}=y$, quae pro casu cognito praebet $a=0$ et $b=2$, nostra solutio dat:

Valores ipsius x	Valores ipsius y
0	2
8	18
144	322
2584	5778
etc.	etc.

Verum hanc formulam diligentius scrutanti patebit, non solum his casibus $\sqrt{(5xx+4)}$ fieri rationalem, sed etiam istis numeris pro x substituendis

$$x=0,\ 1,\ 3,\ 8,\ 21,\ 55,\ 144,\ 377,\ 987,\ \text{etc.}$$

unde solutionum numerus triplicatur. Cujus rei ratio est, quod ad formulam $p=\sqrt{(5qq+1)}$ resolvendam posuimus $q=4$, unde fit $p=9$; quae quidem est simplicissima solutio in numeris integris. At quoniam in scala relationis inest $2p$, ea numeris integris constabit, etiamsi p sit fractio denominatorem habens 2. Hanc ob rem istas simpliciores solutiones nanciscemur, si ponamus $q=\frac{1}{2}$, unde fit $p=\frac{3}{2}$; sicque, ob $\alpha=5$, secundi valores erunt:

$$a'=\frac{3}{2}a\pm\frac{1}{2}b+\frac{1}{20}\beta,\quad b'=\frac{5}{2}a\pm\frac{3}{2}b+\frac{1}{4}\beta$$

ac tertii cum sequentibus per hanc legem suppeditabuntur:

$$a''=3a'-a+\frac{1}{10}\beta,\quad b''=3b'-b,$$

unde nanciscimur hos

valores ipsius x	valores ipsius y
a,	$\pm b$,
$\frac{3}{2}a\pm\frac{1}{2}b+\frac{1}{20}\beta$,	$\frac{5}{2}a\pm\frac{3}{2}b+\frac{1}{4}\beta$,
$\frac{7}{2}a\pm\frac{3}{2}b+\frac{1}{4}\beta$,	$\frac{15}{2}a\pm\frac{7}{2}b+\frac{3}{4}\beta$,
$9a\pm 4b+\frac{4}{5}\beta$,	$20a\pm 9b+2\beta$,
$\frac{47}{2}a\pm\frac{21}{2}b+\frac{9}{4}\beta$,	$\frac{105}{2}a\pm\frac{47}{2}b+\frac{21}{4}\beta$,
$\frac{123}{2}a\pm\frac{55}{2}b+\frac{121}{20}\beta$,	$\frac{275}{2}a\pm\frac{123}{2}b+\frac{55}{4}\beta$,
$161a\pm 72b+16\beta$,	$360a\pm 161b+36\beta$,
etc.	etc.

Atque hinc illae triplo plures solutiones oriuntur, quoties fuerit $a \pm b$ numerus par, ac β vel $= 0$, vel per 20 divisibile.

26. **Scholion 2.** Quandoque ergo plures solutiones in numeris integris reperiuntur, si pro p et q fractiones cum denominatore 2 assumuntur, quod quando in genere eveniat, operae pretium erit investigasse. Plerumque autem hi casus locum non habent, nisi sit vel $\beta = 0$, vel formula ad talem formam reduci possit. Sit ergo proposita formula $\sqrt{(\alpha xx + \gamma)} = y$, cui satisfaciat casus $x = a$ et $y = b$; tum statuatur $p = \frac{m}{2}$ et $q = \frac{n}{2}$, seu quaerantur numeri m et n, ut sit $mm = \alpha nn + 4$ et $m = \sqrt{(\alpha nn + 4)}$. Tum vero solutio prima statim dat secundam:

$$a' = \frac{ma + nb}{2} \quad \text{et} \quad b' = \frac{\alpha na + mb}{2},$$

ubi quidem numeri m et n tam negative, quam affirmative accipi possunt. Denique his binis primis inventis, sequentes per hanc regulam reperientur:

$$a'' = ma' - a \quad \text{et} \quad b'' = mb' - b.$$

In genere autem quilibet numerus pro x satisfaciens continetur hac formula:

$$x = \frac{1}{2\sqrt{\alpha}}(a\sqrt{\alpha} + b)\left(\frac{m + n\sqrt{\alpha}}{2}\right)^{\mu} + \frac{1}{2\sqrt{\alpha}}(a\sqrt{\alpha} - b)\left(\frac{m - n\sqrt{\alpha}}{2}\right)^{\mu},$$

ex qua fit:

$$y = \frac{1}{2}(a\sqrt{\alpha} + b)\left(\frac{m + n\sqrt{\alpha}}{2}\right)^{\mu} - \frac{1}{2}(a\sqrt{\alpha} - b)\left(\frac{m - n\sqrt{\alpha}}{2}\right)^{\mu}.$$

Quoties igitur $ma + nb$ prodierit numerus par, neque tamen m et n sint pares, toties triplo plures solutiones in integris prodeunt, quam methodo praecedente. Hae vero solutiones ita se habebunt:

$$a = a \qquad b = b$$

$$a' = \frac{ma + nb}{2} \qquad b' = \frac{mb + \alpha na}{2}$$

$$a'' = \frac{(mm - 2)a + mnb}{2} \qquad b'' = \frac{(mm - 2)b + \alpha mna}{2}$$

$$a''' = \frac{(m^3 - 3m)a + (mm - 1)nb}{2} \qquad b''' = \frac{(m^3 - 3m)b + \alpha(mm - 1)na}{2}$$

$$a^{IV} = \frac{(m^4 - 4mm + 2)a + (m^3 - 2m)nb}{2} \qquad b^{IV} = \frac{(m^4 - 4mm + 2)b + \alpha(m^3 - 2m)na}{2}$$

$$a^{V} = \frac{(m^5 - 5m^3 + 5m)a + (m^4 - 3m^2 + 1)nb}{2} \qquad b^{V} = \frac{(m^5 - 5m^3 + 5m)b + \alpha(m^4 - 3m^2 + 1)na}{2}$$

etc.

27. **Observatio 1.** Haec altera methodus tum demum plures solutiones in numeris integris suppeditat, quam prior, cum m et n fuerint numeri impares, simulque a et b ambo vel pares, vel impares. Si enim m et n sint numeri pares, p et q erunt integri, et formula $m = \sqrt{(\alpha nn + 4)}$ easdem solutiones praebebit, ac formula $p = \sqrt{(\alpha qq + 1)}$. Deinde si $ma \pm nb$ non fuerit numerus par, valores a', a'' non evadent integri, neque propterea plures solutiones reperiuntur, quam priore methodo, dum adhibetur formula $p = \sqrt{(\alpha qq + 1)}$. Distingui ergo oportet eos casus, quibus formulae $m = \sqrt{(\alpha nn + 4)}$, numeris imparibus pro m et n accipiendis, satisfieri potest, id quod statim patet fieri non posse, si α fuerit numerus formae $4z - 1$, vel etiam hujus $8z + 1$. Quare pro α

alii numeri impares non relinquuntur, nisi qui sint formae $4z+5$. Pro his ergo casibus minimos valores, formulae $m=\sqrt{(ann+4)}$ satisfacientes, sequens tabella exhibet:

Si fuerit	capiatur	eritque	Si fuerit	capiatur	eritque
$a=5$	$n=1$	$m=3$	$a=53$	$n=7$	$m=51$
$a=13$	$n=3$	$m=11$	$a=61$	$n=195$	$m=1523$
$a=21$	$n=1$	$m=5$	$a=69$	$n=75$	$m=623$
$a=29$	$n=5$	$m=27$	$a=77$	$n=1$	$m=9$
$a=37$	$n=$ „	$m=$ „	$a=85$	$n=9$	$m=83$
$a=45$	$n=1$	$m=7$	$a=93$	$n=57$	$m=839$

quaeritur hic ratio, cur casus $a=37$ non recipiat valores impares pro m et n?

Hic igitur patet, si sit $a=37$, non dari numeros impares pro m et n, pro reliquis autem casibus resolutio succedit. Ita si proponatur haec formula $\sqrt{(53xx+28)}=y$, habetur statim $a=1$ et $b=9$. Deinde ob $n=7$ et $m=51$, erit

$$a'=\frac{51+63}{2}=57 \quad \text{et} \quad b'=\frac{371+459}{2}=415,$$

seu etiam $a'=-6$, $b'=-44$, et series recurrentes pro x et y, quarum scala relationis est 51, -1, erunt:

$$x=\text{etc.}\ -307,\ -6,\ 1,\ 57,\ 2906,\ \text{etc.}$$
$$y=\text{etc.}\ \ 2235,\ \ 44,\ 9,\ 415,\ 21156,\ \text{etc.}$$

28. **Observatio 2.** Sufficit autem casus evolvisse, quibus in formula generali $\alpha xx+\beta x+\gamma$ secundus terminus deest, quoniam haec ad talem formam salva numerorum integritate revocari potest. Vulgaris quidem modus, quo ex aequationibus terminus tolli solet, ponendo $x=y-\frac{\beta}{2\alpha}$, hic locum habere nequit, nisi β sit numerus per 2α divisibilis. Verum si $\alpha xx+\beta x+\gamma$ debeat esse quadratum, ponatur $\alpha xx+\beta x+\gamma=yy$, ac multiplicando per 4α prodibit

$$4\alpha\alpha xx+4\alpha\beta x+4\alpha\gamma=4\alpha yy,$$

ideoque

$$4\alpha yy+\beta\beta-4\alpha\gamma=(2\alpha x+\beta)^2.$$

Quaerantur ergo casus, quibus formula $4\alpha yy+\beta\beta-4\alpha\gamma$ fit quadratum, indeque habebuntur valores pro x substituendi, qui formulam $\alpha xx+\beta x+\gamma$ reddant quadratam, scilicet si fuerit $\sqrt{(4\alpha yy+\beta\beta-4\alpha\gamma)}=z$, erit $2\alpha x+\beta=z$, hincque $x=\frac{z-\beta}{2\alpha}$.

Quodsi β fuerit numerus par, puta 2δ, posito:

$$\alpha xx+2\delta x+\gamma=yy, \quad \text{erit} \quad (\alpha x+\delta)^2=\alpha yy+\delta\delta-\alpha\gamma$$

sicque formula $\alpha yy+\delta\delta-\alpha\gamma$ ad quadratum est revocanda, ac si invenimus $\sqrt{(\alpha yy+\delta\delta-\alpha\gamma)}=z$, erit $\alpha x+\delta=z$ et $x=\frac{z-\delta}{\alpha}$, unde plerumque pro x numeri integri reperiuntur; etsi enim forte $\frac{z-\delta}{\alpha}$ non fuerit integer, tamen ex uno valore z cognito, si modo supra tradito alii eliciantur in infinitum, alterni saltem erunt numeri integri. Ex quo perspicuum est, resolutionem formularum quadraticarum radicalium $\sqrt{(\alpha xx+\beta x+\gamma)}$ nulla limitatione affici, etiamsi terminus βx plane omittatur, sicque

totum negotium huc redit, ut formulae hujusmodi $\sqrt{(\alpha xx+\gamma)}$ rationales, et quidem in numeris integris reddantur.

29. **Observatio 3.** Jam annotavi, formulam $\alpha xx+\gamma$ in numeris integris saltem pluribus ac infinitis modis quadratum effici non posse, nisi α sit numerus positivus non quadratus. Existente autem α tali numero, problema non ita resolvi potest, ut pro quocunque numero pro γ assumto, solutio succedat: possent enim utique ejusmodi numeri pro γ dari, ut problema nullam plane solutionem admitteret, atque hanc ob rem postulari unam saltem solutionem cognitam esse debere, quo ipso casus insolubiles exclusi. Verum dato α characteres exhiberi possunt, ex quibus dignosci liceat, utrum numerus γ sit ejusmodi, qui solutionem admittat, nec ne? Ac primo quidem perspicuum est, nullam solutionem locum habere posse, nisi γ sit numerus in tali formula $bb-\alpha aa$ contentus. Dato ergo numero α, formetur series omnium numerorum, tam positivorum, quam negativorum, qui quidem in formula $bb-\alpha aa$ sint contenti; ac nisi γ in hac serie reperiatur, certo pronunciare licet, formulam $\sqrt{(\alpha xx+\gamma)}$ nullo modo rationalem reddi posse: vicissim autem, quoties γ in hac serie comprehenditur, quia tum est $\gamma=bb-\alpha aa$, formula $\alpha xx+\gamma$ fit quadratum, ponendo $x=a$, eritque $\sqrt{(\alpha xx+\gamma)}=b$. Haec igitur series, cujus quasi terminus generalis est $bb-\alpha aa$, primo continebit, sumto $a=0$, omnes numeros quadratos 1, 4, 9, 16, 25, etc. tum vero omnes quadratos per $-\alpha$ multiplicatos, nempe: $-\alpha$, -4α, -9α, -16α, etc. Praeterea si p et q fuerint numeri in hac serie contenti, in ea quoque reperietur eorum productum pq; nam cum sit

$$p=bb-\alpha aa \quad \text{et} \quad q=dd-\alpha cc, \quad \text{erit} \quad pq=(bd\pm\alpha ac)^2-\alpha(bc\pm ad)^2,$$

et ob ambiguitatem signi hoc productum duplici modo est numerus formae $bb-\alpha aa$, ideoque statim habentur duae solutiones $x=bc+ad$ et $x=bc-ad$.

30. **Observatio 4.** Hinc ergo consecuti sumus hoc theorema eximium, quod fundamentum superiorum solutionum in se complectitur:

Si fuerit $\alpha xx+p=yy$ casu $x=a$ et $y=b$, tum vero etiam $\alpha xx+q=yy$ casu $x=c$ et $y=d$, haec formula $\alpha xx+pq=yy$ adimplebitur capiendo

$$x=bc\pm ad \quad \text{et} \quad y=bd\pm\alpha ac.$$

Si enim sit $q=1$ et $dd=\alpha cc+1$, praeterea vero formulae $\alpha xx+p=yy$ satisfiat casu $x=a$ et $y=b$, qui est casus supra pro cognito assumtus, tum eidem formulae satisfacient valores:

$$x=bc\pm ad \quad \text{et} \quad y=bd\pm\alpha ac,$$

unde eadem omnino solutio conficitur, quam supra exhibuimus, atque ex longe diversis principiis elicuimus: quocirca haec postrema investigationis ratio ob concinnitatem et perspicuitatem eo magis est notatu digna. Hic vero accedit, quod haec ratio multo latius pateat, quam praecedens, quippe quae ad casum $q=1$ fuerat adstricta. Demonstratio autem istius theorematis elegantissimi ita brevissime se habebit:

Cum sit $\alpha aa+p=bb$, erit $p=bb-\alpha aa$ et ob $\alpha cc+q=dd$, erit $q=dd-\alpha cc$; hinc erit $pq=(bb-\alpha aa)(dd-\alpha cc)$, quae expressio reducitur ad hanc:

$$pq=(bd\pm\alpha ac)^2-\alpha(bc\pm ad)^2.$$

Quodsi ergo fuerit $x=bc\pm ad$ et $y=bd\pm\alpha ac$, erit $pq=yy-\alpha xx$, ideoque $\alpha xx+pq=yy$. Q. E. D.

31. **Observatio 5.** Cum igitur pro quolibet numero α formulae $\alpha xx + \gamma = yy$, numerus γ debeat esse formae $bb - \alpha aa$, numeri in hac forma contenti diligentius examinari merentur; et quoniam, si inter eos occurrunt numeri p et q, simul quoque eorum productum pq occurrit, praeter numeros quadratos 1, 4, 9, 16, 25, etc. eorumque multipla negativa $-\alpha$, -4α, -9α, -16α, -25α, etc. imprimis numeri primi in hac forma contenti sunt spectandi, quippe ex quibus deinceps per multiplicationem compositi nascuntur.

I. Sit $\alpha = 2$ et numeri primi formae $bb - 2aa$ sunt:

positivi: $+1$, $+2$, $+7$, $+17$, $+23$, $+31$, $+41$, $+47$, $+71$, $+73$, $+79$, $+89$, $+97$, etc.
negativi: -1, -2, -7, -17, -23, -31, -41, -47, -71, -73, -79, -89, -97, etc.

qui praeter $+2$ et -2 omnes in forma $\pm(8n \pm 1)$ continentur.

II. Sit $\alpha = 3$ et numeri primi formae $bb - 3aa$ sunt:

positivi: $+1$, $+13$, $+37$, $+61$, $+73$, $+97$, $+109$, etc.
negativi: -2, -3, -11, -23, -47, -59, -71, -83, -107, etc.

qui praeter -2 et -3 omnes continentur in forma $12n + 1$, siquidem pro n tam numeri positivi, quam negativi capiantur.

III. Sit $\alpha = 5$ et numeri primi formae $bb - 5aa$ sunt:

positivi: $+1$, $+5$, $+11$, $+19$, $+29$, $+31$, $+41$, $+59$, $+61$, $+71$, $+79$, $+89$, $+101$, etc.
negativi: -1, -5, -11, -19, -29, -31, -41, -59, -61, -71, -79, -89, -101, etc.

qui praeter $+5$ et -5, omnes in forma $10n \pm 1$ continentur.

IV. Sit $\alpha = 6$ et numeri primi formae $bb - 6aa$ sunt:

positivi: $+1$, $+3$, $+19$, $+43$, $+67$, $+73$, $+97$, etc.
negativi: -2, -23, -29, -47, -53, -71, -101, etc.

qui, praeter -2 et $+3$, omnes in alterutra harum formarum: $24n + 1$ et $24n - 5$ continentur, sumendo pro n numeros tam negativos, quam positivos.

V. Sit $\alpha = 7$ et numeri primi formae $bb - 7aa$ sunt:

positivi: $+1$, $+2$, $+29$, $+37$, $+53$, $+109$, etc.
negativi: -7, -3, -19, -31, -47, -59, -83, etc.

qui praeter $+2$ et -7 omnes in una harum formarum continentur:

$$28n + 1, \quad 28n + 9, \quad 28n + 25.$$

32. **Observatio 6.** Hinc colligimus, omnes numeros primos in formula $bb - \alpha aa$ contentos simul in quibusdam hujusmodi formulis $-4\alpha n + A$ contineri, dum pro A certi quidam numeri substituuntur. Quod idem etiam hoc modo ostendi potest: ponatur $b = 2\alpha p + r$ et $a = 2q + s$, ac formula $bb - \alpha aa$ transit in hanc:

$$4\alpha\alpha pp + 4\alpha pr + rr - 4\alpha qq - 4\alpha qs - \alpha ss$$

statuatur $\alpha pp + pr - qq - qs = n$ et habebimus:

$$bb - \alpha aa = 4\alpha n + rr - \alpha ss$$

omnes ergo numeri primi formae $bb - aaa$ quoque in hac forma $4an + rr - ass$ continentur; atque ut hi numeri sint primi, r et s ita accipi oportet, ut numerus $rr - ass$ sit vel ipse primus, vel saltem ad $4a$ primus. Primo ergo sumto $s = 0$, pro r successive accipi possunt numeri impares ad a primi, ac si rr fuerit majus quam $4a$, inde $4a$ toties subtrahatur, quoties fieri potest, ut residuum sit minus quam $4a$, et quot hoc modo diversi numeri resultant, ii in formula $4an + A$ loco A collocentur. Deinde etiam simili modo colligantur numeri ex formulis $rr - a$, qui quatenus sunt diversi, ad illos insuper adjiciantur. Non autem opus est, pro s alios numeros praeter unitatem assumere; si enim s esset numerus par, numerus $-ass$ jam in forma $4an$ contineretur, et si s esset impar, numerus $-ass$ haberet formam $-4aN - a$, cujus pars $-4aN$ jam in $4an$ continetur, sicque sufficit pro formulis $4an + A$, quovis casu has $4an + rr$ et $4an + rr - a$ evolvere, eaeque jam omnes numeros primos, qui quidem in formula $bb - aaa$ comprehenduntur, in se complectentur. Num autem vicissim omnes numeri primi, in his formulis $4an + rr$ et $4an + rr - a$ contenti, simul sint numeri formae $bb - aaa$? quaestio est altioris indaginis, quae tamen affirmanda videtur.

33. **Observatio 7.** Quo haec exemplo illustremus, sit $a = 13$, et ex $4an + rr$ et $4an + rr - a$ orientur hae formulae pro numeris primis:

ex $4an + rr$	ex $4an + rr - a$
$52n + 1$	$52n - 9$
$52n + 9$	$52n + 3$
$52n + 25$	$52n + 23$
$52n + 49 = 52n - 3$	$52n + 51 = 52n - 1$
$52n + 81 = 52n - 23$	$52n + 87 = 52n - 17$
$52n + 121 = 52n + 17$	$52n + 131 = 52n - 25$

quae formulae reducuntur ad has:

$$52n \pm 1,\ \ 52n \pm 3,\ \ 52n \pm 9,\ \ 52n \pm 17,\ \ 52n \pm 23,\ \ 52n \pm 25$$

ac numeri primi in his contenti sunt:

$$\pm 1,\ \pm 3,\ \pm 17,\ \pm 23,\ \pm 29,\ \pm 43,\ \pm 53,\ \pm 61,\ \pm 79,\ \pm 101,\ \pm 103,$$

quibus addi debet ± 13; tum vero omnes numeri quadrati; atque si insuper adjiciantur producta ex binis pluribusve horum numerorum, obtinebuntur hoc quidem casu omnes numeri, qui pro γ substituti producunt formulam $13xx + \gamma = yy$ in numeris integris resolubilem; seu quicunque illorum numerorum pro γ accipiatur, unus primo, deinde infiniti numeri integri pro x inveniri possunt, quibus formula $13xx + \gamma$ quadratum reddatur. Omnes enim isti numeri simul in forma $bb - 13aa$ continentur: qui enim huc difficiliores reductu videntur, sunt:

$$-1 = 18^2 - 13.5^2,\quad +13 = 65^2 - 13.18^2,\quad -3 = 7^2 - 13.2^2,\quad +17 = 15^2 - 13.4^2,$$
$$-17 = 10^2 - 13.3^2,\quad -23 = 43^2 - 13.12^2,\quad +29 = 9^2 - 13.2^2,\quad -29 = 32^2 - 13.9^2,$$
$$+43 = 76^2 - 13.21^2,\quad -43 = 3^2 - 13.2^2,\quad +53 = 51^2 - 13.14^2,\quad -53 = 8^2 - 13.3^2,$$
$$+61 = 23^2 - 13.6^2,\quad -61 = 24^2 - 13.7^2,\quad +79 = 14^2 - 13.3^2,\quad -79 = 16^2 - 13.5^2,$$

etc.

Cum ergo sit $-1 = 18^2 - 13.5^2$, si fuerit $+\gamma = bb - 13aa$, erit

$$-\gamma = (18b \pm 65a)^2 - 13(18a \pm 5b)^2,$$

unde casus difficiliores resolvuntur.

Proposita ergo resolvenda hac aequatione $13xx + 43.79 = yy$, cum sit $\gamma = 43.79 = -43.-79$, habebitur per compositionem:

$$\text{I.} \quad \gamma = (14.76 \pm 13.63)^2 - 13(14.21 \pm 3.76)^2,$$

ergo $x = 294 \pm 228$ et $y = 1064 \pm 819$.

$$\text{II.} \quad \gamma = (3.16 \pm 13.10)^2 - 13(2.16 \pm 3.5)^2$$

ergo $x = 32 \pm 15$ et $y = 130 \pm 48$,

unde statim 4 solutiones obtinentur.

34. **Observatio 8.** Verum non semper ex his numeris primis, quos modo investigare docuimus, cum quadratis omnes plane numeri, qui pro γ assumi possunt, reperiuntur, cujus rei exemplum est casus $\alpha = 10$, pro quo valores ipsius γ in hac forma $bb - 10aa$ continentur; iique sunt, tam negative, quam positive sumti:

1, 4, 6, 9, 10, 15, 16, 24, 25, 26, 31, 36, 39, 40, 41, 49, 54, 60, 64, 65, 71, 74, 79, 81, 86, 89, 90, 96, 100, 104, 106, 111, 121, 124, 129, 134, 135, 144, 150, 151, 156, 159, 160, 164, 166, 169, 185, 186, 191, 196, 199, 201, etc.

inter quos numeros occurrunt primo omnes quadrati:

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, etc.

deinde numeri primi 31, 41, 71, 79, 89, 151, 191, 199, etc., qui in his formulis continentur $40n \pm 1$ et $40n \pm 9$, insuperque accedunt producta ex binis pluribusve horum numerorum. Tertio vero, praeter hos, adsunt numeri ex binis numeris primis compositi, qui sunt:

2.3, 2.5, 2.13, 2.37, 2.43, 2.53, 2.67, 2.83, etc.
3.5, 3.13, 3.37, 3.43, 3.53, 3.67, etc.
5.13, 5.37, etc.

At hi numeri primi, quorum semper bini sunt in se multiplicandi, sunt primo 2 et 5, reliqui vero in his formulis continentur $40n \pm 3$ et $40n \pm 13$. Denique etiam secundum regulam generalem adjici debent producta ex binis pluribusve numeris, qui per se satisfaciunt. Ita resolvi poterit haec aequatio: $10xx + 13.53.151 = yy$; nam est $13.53 = bb - 10aa$ existente $b = 27$ et $a = 2$, et $151 = dd - 10cc$; existente $d = 31$ et $c = 9$, hincque

$$13.53.151 = (bd \pm 10ac)^2 - 10(ad \pm bc)^2$$

et $x = ad \pm bc$ et $y = bd \pm 10ac$.

Deinde cum etiam sit $-13.53 = BB - 10AA$ et $-151 = DD - 10CC$, hinc duae aliae solutiones reperiuntur. Cum autem sit $-1 = 3^2 - 10.1^2$, si fuerit $\gamma = bb - 10aa$, erit

$$-\gamma = (3b \pm 10a)^2 - 10(3a \pm b)^2.$$

Solutiones autem hinc oriundae sunt:

$$x = 181, \; y = 657, \quad \Big| \quad x = 305, \; y = 1017, \quad \Big| \quad x = 307, \; y = 1023,$$

duae enim inter se conveniunt, ita ut hinc tres tantum reperiantur.

35. **Observatio 9.** Hoc ergo casu $\alpha = 10$ pro γ triplicis generis numeros primitivos invenimus, primo scilicet numeros quadratos omnes, deinde certos numeros primos in formulis $40n \pm 1$ et $40n \pm 9$ contentos, tertio autem producta ex binis certis numeris primis, qui sunt 2, 5 et reliqui ex his formulis $40n \pm 3$ et $40n \pm 13$ petendi, atque ex hoc demum triplici ordine omnes numeri pro γ idonei formantur, ut huic aequationi $10xx \pm \gamma = yy$ satisfieri possit. Ipsi autem numeri primi in formulis $40n \pm 3$ et $40n \pm 13$ contenti non conveniunt, quia non sunt formae $bb - 10aa$, sed tamen hi numeri omnes sunt formae $2bb - 5aa$; uti etiam duo iis jungendi 2 et 5. Manifestum autem est, si habeantur duo numeri hujusmodi $2bb - 5aa$ et $2dd - 5cc$, eorum productum fore $= (2bd \pm 5ac)^2 - 10(bc \pm ad)^2$, ideoque pro γ adhiberi posse. Hujusmodi igitur producta binorum numerorum primorum, qui ipsi non satisfaciunt, occurrere nequeunt, si α fuerit numerus primus, sed tantum, uti hic usu venit, si α fuerit numerus compositus; quod tamen etiam non semper locum habet, uti vidimus casu $\alpha = 6 = 2.3$, quo numeri formae $3bb - 2aa$ conveniunt cum numeris formae $bb - 6aa$. Quodsi ergo in genere fuerit $\alpha = pq$, et aequatio $pqxx + \gamma = yy$ resolvi debeat, numerus γ vel esse debet numerus quadratus, vel primus formae $bb - pqaa$, vel productum ex duobus numeris primis formae $pbb - qaa$, propterea quod hujusmodi productum est:

$$(pbb - qaa)(pdd - qcc) = (pbd \pm qac)^2 - pq(bc \pm ad)^2.$$

Nisi ergo tales numeri primi jam ipsi $pbb - qaa$ in forma $bb - pqaa$ contineantur, tertius ille ordo numerorum ex binis numeris primis conflatorum accedit. Quemadmodum deinde numeri primi solitarii continentur in formulis

$$4pqn + rr \quad \text{et} \quad 4pqn + rr - pq$$

ita numeri primi alteri combinandi ex formula hac:

$$4pqn + prr - qss$$

derivari debent.

36. **Exempl. 1.** *Investigentur omnes valores idonei ipsius γ, ut haec aequatio $30xx + \gamma = yy$ resolutionem admittat.*

Primo quidem pro γ assumi possunt omnes numeri quadrati, deinde omnes numeri primi in his formis $120n + rr$ et $120n + rr - 30$ contenti, quae reducuntur ad has:

$$120n + 1, \quad 120n + 49, \quad 120n + 19, \quad 120n - 29, \quad \text{cum} \; -5$$

unde oriuntur hi numeri primi infra 200

positivi: $+19, \; +139,$

et negativi: $-5, \; -29, \; -71, \; -101, \; -149, \; -191.$

Tertio ob $\alpha = 2.3.5$, sumi possunt producta trinorum primorum, qui contineantur vel ambo in una harum formularum:

$$\text{I. } 120n + 2rr - 15ss, \quad \text{II. } 120n + 3rr - 10ss; \quad \text{III. } 120n + 5rr - 6ss,$$

harum autem binae priores eosdem numeros primos dant, qui sunt $+2$, $+3$, et reliqui in his formulis continentur:

$$120n - 7, \quad 120n - 13, \quad 120n + 17, \quad 120n - 37,$$

unde nascuntur hi numeri primi infra 200

positivi: $+2$, $+3$, $+17$, $+83$, $+107$, $+113$, $+137$,
negativi: -7, -13, -37, -103, -127,

quorum binorum producta pro γ capienda sunt:

$+6$, $+34$, $+51$, $+91$, $+166$,
-14, -21, -26, -39, -74, -111, -119.

Tertia autem formula continet numerum primum $+5$, cum his formis:

$$120n - 1, \quad 120n - 19, \quad 120n + 29, \quad 120n - 49,$$

unde nascuntur hi numeri primi infra 200

positivi: $+5$, $+29$, $+71$, $+101$, $+149$, $+191$,
negativi: -1, -19, -139.

At ex horum combinatione iidem nascuntur numeri, qui jam ex numeris primis primitivis oriuntur. Quocirca omnes numeri, qui pro γ substitui possunt, erunt infra 200:

$+1$, $+4$, $+9$, $+16$, $+25$, $+36$, $+49$, $+64$, $+81$, $+100$, $+121$, $+144$, $+169$, $+196$
-5, $+19$, -29, -71, -101, $+139$, -149, -191,
$+6$, -14, -21, -26, -34. -39, $+51$, -74, $+91$, -111, -119, $+166$,
-20, $+24$, -30, -45, $+54$, -56, $+70$, $+76$, -80, -84, -95, $+96$, -104, $+105$,
$+114$, -116, -125, -126, $+130$, $+136$, $+145$, $+150$, -156, -170, $+171$, -189, $+195$,

reliqui autem numeri omnes pro γ assumti reddent problema impossibile.

37. **Exempl. 2.** *Resolvere in numeris integris aequationem*

$$5xx + 11.19.29 = yy.$$

Quia est $\alpha = 5$ et $\gamma = 11.19.29$, factores hi cum forma $bb - 5aa$ conveniunt, et singuli in ea contineri deprehenduntur: nam

$$\left.\begin{array}{llll} \text{pro} & 11 & \text{est} & b = 4, \quad a = 1 \\ „ & 19 & „ & b = 8, \quad a = 3 \\ „ & 29 & „ & b = 7, \quad a = 2 \end{array}\right\} \text{ unde etiam producta ex binis in eadem forma continentur,}$$

$$\text{pro } 11.19 \text{ est } \begin{Bmatrix} b = 17, & a = 4 \\ b = 47, & a = 20 \end{Bmatrix} \text{ ergo tertium adjungendo}$$

$$\text{pro } 11.19.29 \text{ est } \begin{cases} b = 79, & a = 6 \\ b = 159, & a = 62 \\ b = 129, & a = 46 \\ b = 529, & a = 234. \end{cases}$$

Cum jam sit $1 = 9^2 - 5.4^2$, seu $b = 9$ et $a = 4$ pro 1, hae formulae insuper per 1 multiplicatae duplicabuntur, fietque pro 11.19.29

$b = 591, \quad a = 262$	$b = 241, \quad a = 102$
$b = 831, \quad a = 370$	$b = 2081, \quad a = 930$
$b = 191, \quad a = 78$	$b = 81, \quad a = 10$
$b = 2671, \quad a = 1194$	$b = 9441, \quad a = 4222$

Hinc ergo jam duodecim solutiones problematis sumus nacti, quae sunt:

I. $x = 6, \quad y = 79$	VII. $x = 234, \quad y = 529$
II. $x = 10, \quad y = 81$	VIII. $x = 262, \quad y = 591$
III. $x = 46, \quad y = 129$	IX. $x = 370, \quad y = 831$
IV. $x = 62, \quad y = 159$	X. $x = 930, \quad y = 2081$
V. $x = 78, \quad y = 191$	XI. $x = 1194, \quad y = 2671$
VI. $x = 102, \quad y = 241$	XII. $x = 4222, \quad y = 9441$

ex quibus porro cum formula $1 = 9^2 - 5.4^2$ conjungendis infinitae novae eaeque omnes elicientur: ex secunda scilicet prodit

$x = 414$, $y = 929$; et ex sexta $x = 1882$, $y = 4209$; ex quinta $x = 1466$, $y = 3279$; ex octava $x = 4722$, $y = 10559$;

sicque jam sedecim solutiones sumus adepti.

38. **Conclusio.** His expositis non amplius coacti sumus, proposita hujusmodi aequatione $axx + \gamma = yy$, primum quasi divinando unum casum satisfacientem anquirere, sed numerum γ examinando secundum formulas modo traditas statim pronunciare possumus, utrum aequatio resolutionem admittat, nec ne? ac si admittit, per eadem principia unam saltem solutionem elicere licebit, quod quidem promte fieri poterit, si numerus γ fuerit resolubilis in factores non nimis magnos. Verum si numerus γ sit primus ac praegrandis, judicium quidem solubilitatis aeque est facile, at inventio unius solutionis majorem laborem requirit. Veluti si proponatur $30xx + 1459 = yy$, quia 1459 est numerus primus formae $120n + 19$, aequatio est resolubilis; verum ei satisfieri sumendo $x = 39$ et $y = 217$ non tam facile investigatur. Investigatio tamen sublevatur, si statuamus $y = 30z \pm 7$, unde fit $xx = 30zz \pm 14z - 47$, et jam citius reperiemus $z = 7$ et $x = 39$, unde prodit $y = 217$. At si ponamus $y = 30z \pm 13$, fit $xx = 30zz \pm 26z - 43$, promtiusque invenitur $x = 5$ et $y = 47$. Verum in numeris multo majoribus labor evadit insuperabilis, methodusque certa adhuc desideratur negotium conficiendi: deinde etiam quod omnes numeri primi, in supra allatis formulis $4an + A$ contenti, simul sint numeri hujus formae $bb - aaa$, ad eas propositiones pertinet, quas veras credimus, etiamsi demonstrare non valeamus. In quo cum eximia pars theoriae numerorum versetur, qui hujus generis problemata diligentius perscrutari voluerit, nullum est dubium, quin non contemnendas veritates sit eruturus; ob eandemque causam confido haec ipsa, quae hic attuli, usu non esse caritura: ea ipsa enim, quae adhuc sunt incognita, accuratius exposuisse non parum juvabit.

XXIII.

De usu novi algorithmi in problemate Pelliano solvendo.

(N. Comment. XI. 1765 p. 28. Exhib. 1759 Oct. 15.)

1. Quicunque numeri integri pro litteris l, m et n assumantur, innumerabiles quoque numeri integri pro x inveniri possunt, quibus haec formula:

$$lxx + mx + n \text{ reddatur quadratum,}$$

siquidem sequentes conditiones habeant locum:

1) ut l sit numerus positivus non quadratus,

2) ut pro x unus saltem valor sit cognitus.

Nam si l est numerus vel negativus, vel quadratus, manifestum est, infinitas solutiones in numeris integris exhiberi non posse, etiamsi una innotuerit. Tum vero etiam evenire potest, ut formula $lxx + mx + n$ naturae quadrati prorsus adversetur, uti fit hoc casu $3xx + 2$. Verum statim atque unica solutio habetur, semper innumerabiles invenire licet.

2. Quare si statuamus:

$$lxx + mx + n = yy,$$

unusque casus constet, quo huic conditioni satisfiat ita ut posito $x = a$, prodeat

$$laa + ma + n = bb$$

sicque sumto $x = a$ obtineatur $y = b$; regula, cujus ope plures imo infinitae solutiones elici possunt, ita se habet:

Primo ex dato numero l duo hujusmodi numeri p et q investigentur, ut sit

$$pp = lqq + 1, \quad \text{seu} \quad p = \sqrt{(lqq + 1)},$$

quibus inventis ex solutione primo cognita statim eruitur haec nova:

$$x = pa + qb + \frac{m(p-1)}{2l}, \quad \text{unde fit}$$

$$y = pb + lqa + \frac{mq}{2},$$

ex qua deinceps simili modo aliae derivantur. Si enim hos valores loco a et b substituamus, nascitur tertia solutio ista:

$$x = (2pp - 1)a + 2pqb + mqq \quad \text{et}$$

$$y = (2pp - 1)b + 2lpqa + mpq,$$

quae certe est in numeris integris, si forte praecedentes adhuc fuerint fracti.

3. Cum igitur hoc modo continuo novae solutiones inveniri queant, ad calculi compendium plurimum juvat notasse, continuos istos valores, tam ipsius x, quam ipsius y, secundum seriem

recurrentem progredi, cujus singuli termini per binos praecedentes certa et constante lege determinentur. Scilicet si fuerint valores hi continuo progredientes:

ipsius x . . . . a . . . . P, Q, R, S, etc.

Ipsius y . . . . b . . . . $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, $\mathfrak{S}$, etc.

erit per legem seriei recurrentis:

$$R = 2pQ - P + \frac{m(p-1)}{l} \qquad \mathfrak{R} = 2p\mathfrak{Q} - \mathfrak{P}$$

$$S = 2pR - Q + \frac{m(p-1)}{l} \qquad \mathfrak{S} = 2p\mathfrak{R} - \mathfrak{Q}.$$

Atque hinc isti valores expressionibus generalibus comprehendi possunt, quae ita se habent:

$$x = \frac{2la + m + 2b\sqrt{l}}{4l}(p + q\sqrt{l})^{\mu} + \frac{2la + m - 2b\sqrt{l}}{4l}(p + q\sqrt{l})^{\mu} - \frac{m}{2l}$$

$$y = \frac{2la + m + 2b\sqrt{l}}{4\sqrt{l}}(p + q\sqrt{l})^{\mu} - \frac{2la - m + 2b\sqrt{l}}{4\sqrt{l}}(p - q\sqrt{l})^{\mu}$$

unde quicunque numeri integri exponenti μ tribuantur, semper valores rationales pro x et y resultant.

4. Haec autem investigatio multo latius ita potest extendi, ut proposita inter binos numeros x et y hujusmodi aequatione:

$$Axx + 2Bxy + Cyy + 2Dx + 2Ey + F = 0$$

omnes solutiones in numeris rationalibus et integris sint eruendae. Hic quidem pariter necesse est, unam solutionem esse cognitam, quae sit $x = a$ et $y = b$, ita ut sit

$$Aaa + 2Bab + Cbb + 2Da + 2Eb + F = 0.$$

Tum vero quaerantur bini numeri p et q, ut sit

$$pp = (BB - AC)qq + 1$$

quod quidem fieri nequit, nisi sit $BB > AC$. Atque nova solutio ita erit comparata:

$$x = a(p + Bq) + bCq + Eq + \frac{BE - CD}{BB - AC}(p - 1)$$

$$y = b(p - Bq) - aAq - Dq + \frac{BD - AE}{BB - AC}(p - 1)$$

unde per eandem legem continuo plures elicere licet.

5. Haec ideo in medium afferre est visum, ut intelligatur, ad omnes hujus generis resolutiones id omnino requiri, ut proposito quocunque numero integro positivo non quadrato l, ejusmodi binos numeros pariter integros p et q inveniri oporteat, ut sit $pp = lqq + 1$, seu $p = \sqrt{(lqq + 1)}$. Atque hoc est illud problema olim quidem maxime celebratum, a solutionis ingeniosissimae auctore **Pellianum** vocatum, quo pro quovis hujusmodi numero l numerus quadratus qq requiritur, qui per l multiplicatus adjuncta unitate fiat quadratus. In fractis quidem haec quaestio nullam haberet difficultatem, cum sumto $q = \frac{2rs}{lss - rr}$, fiat $p = \frac{lss + rr}{lss - rr}$; verum quia numeri integri desiderantur, negotium iterum eo revocatur, ut denominator $lss - rr$ in unitatem abeat.

6. Etiamsi autem solutio Pelliana hujus problematis sit elegantissima, tamen saepenumero tam operosis calculis implicatur, qui non minus taedii quam laboris creare solent. Cum igitur

observassem, algorithmum illum novum, cujus nuper indolem exposui(*), ad hos calculos, quibus hic est opus, contrahendos, insignia subsidia suppeditare, praeclarius certe specimen exhibere vix licebit, quo usus istius algorithmi illustretur et commendetur. Ubi id imprimis notatu dignum occurrit, quod totum compendium inde subministratum potissimum idoneorum signorum usu contineatur.

7. Operationes, quibus Pellius est usus, aliunde quidem satis sunt notae, egoque jam eas alia occasione fusius descripsi; ex quo eo minus opus est, ut iis denuo explicandis hic immoror, cum totam analysin hic longe alia ratione sim instituturus. Ejus scilicet principium ex hoc fonte haurio, quod cum sit $pp = lqq + 1$, proxime fiat $\frac{p}{q} = \sqrt{l}$, ex quo manifestum est, $\frac{p}{q}$ ejusmodi esse fractionem, quae valorem irrationalem $\sqrt{l}$ tam prope exprimat, seu eum tam parum excedat, ut id, nisi majoribus numeris adhibendis, accuratius fieri nequeat. Quod problema, olim feliciter a Wallisio solutum, equidem quoque jam dudum per fractiones continuas multo commodius expedivi.

8. Quo ergo hoc argumentum luculentius et ordine pertractem, primum radicem quadratam ex quovis numero in fractionem continuam evolvere docebo, idque methodo quam minime molesta. Deinde ostendam, quomodo inde fractiones $\frac{p}{q}$ valorem irrationalem $\sqrt{l}$ proxime exprimentes formari debeant, in subsidium vocato algorithmo novo supra explicato. Tum vero facile patebit, quomodo hinc numeros p et q definiri oporteat, ut fiat $pp = lqq + 1$. Denique tabulam subjungam, in qua pro omnibus numeris l, centenarium non superantibus, numeri bini p et q exhibentur.

De evolutione radicum quadratarum per fractiones continuas.

9. Operationes in hunc finem constituendae in exemplo facillime explicabuntur. Sit igitur proposita radix quadrata ex numero 13, et cum radix rationalis proxime minor sit 3, statuo $\sqrt{13} = 3 + \frac{1}{a}$. Hinc colligitur

$$a = \frac{1}{\sqrt{13} - 3} = \frac{\sqrt{13} + 3}{4}$$

cujus valor in integris proxime minor est 1, quod inde patet, si 3 loco $\sqrt{13}$ scribatur. Pono itaque

$$a = \frac{\sqrt{13} + 3}{4} = 1 + \frac{1}{b}, \text{ hincque}$$

$$b = \frac{4}{\sqrt{13} - 1} = \frac{4(\sqrt{13} + 1)}{12} = \frac{\sqrt{13} + 1}{3} = 1 + \frac{1}{c},$$

$$\text{ergo} \quad c = \frac{3}{\sqrt{13} - 2} = \frac{3(\sqrt{13} + 2)}{9} = \frac{\sqrt{13} + 2}{3} = 1 + \frac{1}{d},$$

$$\text{ergo} \quad d = \frac{3}{\sqrt{13} - 1} = \frac{3(\sqrt{13} + 1)}{12} = \frac{\sqrt{13} + 1}{4} = 1 + \frac{1}{e},$$

$$\text{ergo} \quad e = \frac{4}{\sqrt{13} - 3} = \frac{4(\sqrt{13} + 3)}{4} = \sqrt{13} + 3 = 6 + \frac{1}{f},$$

$$\text{ergo} \quad f = \frac{1}{\sqrt{13} - 3} = \frac{\sqrt{13} + 3}{4} = 1 + \frac{1}{g},$$

atque hic operationem abrumpere licet, quia valor f ipsi a aequalis prodiit, ideoque sequentes eodem ordine repetuntur. Sicque invenimus esse

(*) N. Comm. IX. pag. 53.

$$\sqrt{13} = 3 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\text{etc.}}}}}}}}}}$$

10. Quo indoles harum operationum melius perspiciatur, aliud exemplum, prolixiorem calculum postulans, adjungam. Proposita scilicet sit $\sqrt{61}$, cujus valor proxime minor cum sit 7, pono $\sqrt{61} = 7 + \frac{1}{a}$, et operationes sequenti modo erunt instituendae:

I. $a = \frac{1}{\sqrt{61}-7} = \frac{\sqrt{61}+7}{12} = 1 + \frac{1}{b}$,

II. $b = \frac{12}{\sqrt{61}-5} = \frac{12(\sqrt{61}+5)}{36} = \frac{\sqrt{61}+5}{3} = 4 + \frac{1}{c}$,

III. $c = \frac{3}{\sqrt{61}-7} = \frac{3(\sqrt{61}+7)}{12} = \frac{\sqrt{61}+7}{4} = 3 + \frac{1}{d}$,

IV. $d = \frac{4}{\sqrt{61}-5} = \frac{4(\sqrt{61}+5)}{36} = \frac{\sqrt{61}+5}{9} = 1 + \frac{1}{e}$,

V. $e = \frac{9}{\sqrt{61}-4} = \frac{9(\sqrt{61}+4)}{45} = \frac{\sqrt{61}+4}{5} = 2 + \frac{1}{f}$,

VI. $f = \frac{5}{\sqrt{61}-6} = \frac{5(\sqrt{61}+6)}{25} = \frac{\sqrt{61}+6}{5} = 2 + \frac{1}{g}$,

VII. $g = \frac{5}{\sqrt{61}-4} = \frac{5(\sqrt{61}+4)}{45} = \frac{\sqrt{61}+4}{9} = 1 + \frac{1}{h}$,

VIII. $h = \frac{9}{\sqrt{61}-5} = \frac{9(\sqrt{61}+5)}{36} = \frac{\sqrt{61}+5}{4} = 3 + \frac{1}{i}$,

IX. $i = \frac{4}{\sqrt{61}-7} = \frac{4(\sqrt{61}+7)}{12} = \frac{\sqrt{61}+7}{3} = 4 + \frac{1}{k}$,

X. $k = \frac{3}{\sqrt{61}-5} = \frac{3(\sqrt{61}+5)}{36} = \frac{\sqrt{61}+5}{12} = 1 + \frac{1}{l}$,

XI. $l = \frac{12}{\sqrt{61}-7} = \frac{12(\sqrt{61}+7)}{12} = \sqrt{61}+7 = 14 + \frac{1}{m}$,

XII. $m = \frac{1}{\sqrt{61}-7}$,

ergo $m = a$, hincque porro $n = b$, $o = c$, etc. Ex quo indices pro fractione continua erunt: 7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, 4, 3, 1, 2, etc. neque opus est ipsam fractionem continuam hic exhibere.

11. Adhuc aliud exemplum adjecisse juvabit, ubi indicum numerus, antequam iidem recurrunt, fit impar. Esto hoc exemplum: $\sqrt{67} = 8 + \frac{1}{a}$, et operationes sequentes institui oportebit:

I $a = \frac{1}{\sqrt{67}-8} = \frac{\sqrt{67}+8}{3} = 5 + \frac{1}{b}$,

II. $b = \frac{3}{\sqrt{67}-7} = \frac{3(\sqrt{67}+7)}{18} = \frac{\sqrt{67}+7}{6} = 2 + \frac{1}{c}$,

III. $c = \frac{6}{\sqrt{67}-5} = \frac{6(\sqrt{67}+5)}{42} = \frac{\sqrt{67}+5}{7} = 1 + \frac{1}{d}$,

$$\text{IV.} \quad d = \frac{7}{\sqrt{67}-2} = \frac{7(\sqrt{67}+2)}{63} = \frac{\sqrt{67}+2}{9} = 1 + \frac{1}{e},$$

$$\text{V.} \quad e = \frac{9}{\sqrt{67}-7} = \frac{9(\sqrt{67}+7)}{18} = \frac{\sqrt{67}+7}{2} = 7 + \frac{1}{f},$$

$$\text{VI.} \quad f = \frac{2}{\sqrt{67}-7} = \frac{2(\sqrt{67}+7)}{18} = \frac{\sqrt{67}+7}{9} = 1 + \frac{1}{g},$$

$$\text{VII.} \quad g = \frac{9}{\sqrt{67}-2} = \frac{9(\sqrt{67}+2)}{63} = \frac{\sqrt{67}+2}{7} = 1 + \frac{1}{h},$$

$$\text{VIII.} \quad h = \frac{7}{\sqrt{67}-5} = \frac{7(\sqrt{67}+5)}{42} = \frac{\sqrt{67}+5}{6} = 2 + \frac{1}{i},$$

$$\text{IX.} \quad i = \frac{6}{\sqrt{67}-7} = \frac{6(\sqrt{67}+7)}{18} = \frac{\sqrt{67}+7}{3} = 5 + \frac{1}{k},$$

$$\text{X.} \quad k = \frac{3}{\sqrt{67}-8} = \frac{3(\sqrt{67}+8)}{3} = \sqrt{67}+8 = 16 + \frac{1}{l},$$

$$\text{XI.} \quad l = \frac{1}{\sqrt{67}-8},$$

ergo $l = a$, indeque indices b, c, d, etc. ordine recurrunt: quare indices fractionis continuae quaesitae sunt:

8, 5, 2, 1, 1, 7, 1, 1, 2, 5, 16, 5, 2, 1, 1, 7, 1, 1, 2, 5, 16, etc.

12. His exemplis probe perpensis, poterimus jam in genere operationes describere, quibus pro cujusvis numeri radice quadrata fractio continua ipsi aequalis, seu indices eam constituentes, inveniuntur. Sit scilicet numerus propositus $= z$, ejusque radix integra proxime minor $= v$, vera autem hac fractione continua exprimatur:

$$\sqrt{z} = v + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \text{etc.}}}}}$$

cujus indices a, b, c, d, etc. post primum v, per se cognitum, sequentibus operationibus reperiuntur:

	Capiatur	tum vero	eritque
I.	$A = v$	$\alpha = z - AA = z - vv$	$a < \frac{v+A}{\alpha}$
II.	$B = \alpha a - A$	$\beta = \frac{z-BB}{\alpha} = 1 + a(A - B)$	$b < \frac{v+B}{\beta}$
III.	$C = \beta b - B$	$\gamma = \frac{z-CC}{\beta} = \alpha + b(B - C)$	$c < \frac{v+C}{\gamma}$
IV.	$D = \gamma c - C$	$\delta = \frac{z-DD}{\gamma} = \beta + c(C - D)$	$d < \frac{v+D}{\delta}$
V.	$E = \delta d - D$	$\varepsilon = \frac{z-EE}{\delta} = \gamma + d(D - E)$	$e < \frac{v+E}{\varepsilon}$

etc.

ubi in postrema columna signum $<$ indicat, pro litteris a, b, c, d, etc. sumi debere numeros integros proxime minores fractionibus adjectis, nisi hae fractiones ipsae in numeros integros abeant, quo casu hi ipsi erunt indices.

13. Pro indicibus igitur a, b, c, d, etc. eliciendis binas alias numerorum series investigari oportet, quarum priorem litteris majusculis A, B, C, D, etc. posteriorem vero graecis α, β, γ, δ, etc. designavi. Circa priores numeros observo, eos numerum v nunquam superare posse, eorum quidem primus est $A = v$, at cum sit $a < \frac{v+A}{\alpha}$, erit $a\alpha - A < v$, ideoque $B < v$, vel ad summum $B = v$, quo casu fit $\beta = 1$ et $b = 2v$. Deinde ob $b < \frac{v+B}{\beta}$, est $b\beta - B = C < v$, similique modo $D \leqq v$, $E < v$, etc. ita ut horum numerorum nullus ipso v major prodire possit. Deinde patet, praeter casus, quibus graecarum litterarum quaepiam fit unitas, indices a, b, c, etc. omnes ipso v majores esse non posse, quandoquidem in fractionibus $\frac{v+B}{\beta}$, $\frac{v+C}{\gamma}$ etc. numeratores non excedere possunt $2v$, denominatores vero ad minimum sint $= 2$. Denique cum fuerit perventum ad indicem $= 2v$, sequentes iterum prodeunt a, b, c, d, etc.

14. Illustremus etiam has operationes nonnullis exemplis.

I. Sit $z = 31$, erit $v = 5$.

$A = 5$,	$\alpha = 6$,	$a < \frac{10}{6} = 1$,
$B = 6 - 5 = 1$,	$\beta = 1 + 1.4 = 5$,	$b < \frac{6}{5} = 1$,
$C = 5 - 1 = 4$,	$\gamma = 6 - 1.3 = 3$,	$c < \frac{9}{3} = 3$,
$D = 9 - 4 = 5$,	$\delta = 5 - 3.1 = 2$,	$d < \frac{10}{2} = 5$,
$E = 10 - 5 = 5$,	$\varepsilon = 3 - 5.0 = 3$,	$e < \frac{10}{3} = 3$,
$F = 9 - 5 = 4$,	$\zeta = 2 + 3.1 = 5$,	$f < \frac{9}{5} = 1$,
$G = 5 - 4 = 1$,	$\eta = 3 + 1.3 = 6$,	$g < \frac{6}{6} = 1$,
$H = 6 - 1 = 5$,	$\vartheta = 5 - 1.4 = 1$,	$h < \frac{10}{1} = 10$.

II. Sit $z = 46$, erit $v = 6$.

$A = 6$,	$\alpha = 10$,	$a < \frac{12}{10} = 1$,
$B = 10 - 6 = 4$,	$\beta = 1 + 1.2 = 3$,	$b < \frac{10}{3} = 3$,
$C = 9 - 4 = 5$,	$\gamma = 10 - 3.1 = 7$,	$c < \frac{11}{7} = 1$,
$D = 7 - 5 = 2$,	$\delta = 3 + 1.3 = 6$,	$d < \frac{8}{6} = 1$,
$E = 6 - 2 = 4$,	$\varepsilon = 7 - 1.2 = 5$,	$e < \frac{10}{5} = 2$,
$F = 10 - 4 = 6$,	$\zeta = 6 - 2.2 = 2$,	$f < \frac{12}{2} = 6$,
$G = 12 - 6 = 6$,	$\eta = 5 - 6.0 = 5$,	$g < \frac{12}{5} = 2$,
$H = 10 - 6 = 4$,	$\vartheta = 2 + 2.2 = 6$,	$h < \frac{10}{6} = 1$,

$J = 6 - 4 = 2,\qquad \iota = 5 + 1.2 = 7,\qquad i < \frac{8}{7} = 1,$

$K = 7 - 2 = 5,\qquad \varkappa = 6 - 1.3 = 3,\qquad k < \frac{11}{3} = 3,$

$L = 9 - 5 = 4,\qquad \lambda = 7 + 3.1 = 10,\qquad l < \frac{10}{10} = 1,$

$M = 10 - 4 = 6,\qquad \mu = 3 - 1.2 = 1,\qquad m < \frac{12}{1} = 12.$

III. Sit $z = 54$ erit $v = 7$.

$A = 7,\qquad \alpha = 5,\qquad a < \frac{14}{5} = 2,$

$B = 10 - 7 = 3,\qquad \beta = 1 + 2.4 = 9,\qquad b < \frac{10}{9} = 1,$

$C = 9 - 3 = 6,\qquad \gamma = 5 - 1.3 = 2,\qquad c < \frac{13}{2} = 6,$

$D = 12 - 6 = 6,\qquad \delta = 9 + 6.0 = 9,\qquad d < \frac{13}{9} = 1,$

$E = 9 - 6 = 3,\qquad \varepsilon = 2 + 1.3 = 5,\qquad e < \frac{10}{5} = 2,$

$F = 10 - 3 = 7,\qquad \zeta = 9 - 2.4 = 1,\qquad f < \frac{14}{1} = 14.$

15. Tabulam ergo hic subjungam, pro singulorum numerorum radicibus quadratis indices continentem, ex quibus fractiones continuae ipsis aequales formari queant. Simul vero litterarum graecarum singulis convenientium valores subscripti reperiuntur.

Numeri surdi	Indices	Numeri surdi	Indices
$\sqrt{2}$	1, 2, 2, 2 etc. 1 1 1 1	$\sqrt{15}$	3, 1, 6, 1, 6, 1, 6 etc. 1 6 1 6 1 6 1
$\sqrt{3}$	1, 1, 2, 1, 2, 1, 2 etc. 1 2 1 2 1 2 1	$\sqrt{17}$	4, 8, 8, 8, 8 etc. 1 1 1 1 1
$\sqrt{5}$	2, 4, 4, 4 etc. 1 1 1 1	$\sqrt{18}$	4, 4, 8, 4, 8, 4, 8, 4, 8 etc. 1 2 1 2 1 2 1 2 1
$\sqrt{6}$	2, 2, 4, 2, 4, 2, 4 etc. 1 2 1 2 1 2 1	$\sqrt{19}$	4, 2, 1, 3, 1, 2, 8, 2, 1, 3, 1, 2, 8 etc. 1 3 5 2 5 3 1 3 5 2 5 3 1
$\sqrt{7}$	2, 1, 1, 1, 4, 1, 1, 1, 4 etc. 1 3 2 3 1 3 2 3 1	$\sqrt{20}$	4, 2, 8, 2, 8, 2, 8, 2, 8 etc. 1 4 1 4 1 4 1 4 1
$\sqrt{8}$	2, 1, 4, 1, 4, 1, 4 ete. 1 4 1 4 1 4 1	$\sqrt{21}$	4, 1, 1, 2, 1, 1, 8, 1, 1, 2, 1, 1, 8 etc. 1 5 4 3 4 5 1 5 4 3 4 5 1
$\sqrt{10}$	3, 6, 6, 6 etc. 1 1 1 1	$\sqrt{22}$	4, 1, 2, 4, 2, 1, 8, 1, 2, 4, 2, 1, 8 etc. 1 6 3 2 3 6 1 6 3 2 3 6 1
$\sqrt{11}$	3, 3, 6, 3, 6, 3, 6 etc. 1 2 1 2 1 2 1	$\sqrt{23}$	4, 1, 3, 1, 8, 1, 3, 1, 8 etc. 1 7 2 7 1 7 2 7 1
$\sqrt{12}$	3, 2, 6, 2, 6, 2, 6 etc. 1 3 1 3 1 3 1	$\sqrt{24}$	4, 1, 8, 1, 8, 1, 8 etc. 1 8 1 8 1 8 1
$\sqrt{13}$	3, 1, 1, 1, 1, 6, 1, 1, 1, 1, 6 etc. 1 4 3 3 4 1 4 3 3 4 1	$\sqrt{26}$	5, 10, 10, 10 etc. 1 1 1 1
$\sqrt{14}$	3, 1, 2, 1, 6, 1, 2, 1, 6 etc. 1 5 2 5 1 5 2 5 1	$\sqrt{27}$	5, 5, 10, 5, 10, 5, 10 etc. 1 2 1 2 1 2 1

Numeri surdi	Indices
√28	5, 3, 2, 3, 10, 3, 2, 3, 10 etc. 1 3 4 3 1 3 4 3 1
√29	5, 2, 1, 1, 2, 10, 2, 1, 1, 2, 10 etc. 1 4 5 5 4 1 4 5 5 4 1
√30	5, 2, 10, 2, 10, 2, 10, 2, 10 etc. 1 5 1 5 1 5 1 5 1
√31	5, 1, 1, 3, 5, 3, 1, 1, 10 etc. 1 6 5 3 2 3 5 6 1
√32	5, 1, 1, 1, 10, 1, 1, 1, 10 etc. 1 7 4 7 1 7 4 7 1
√33	5, 1, 2, 1, 10, 1, 2, 1, 10 etc. 1 8 3 8 1 8 3 8 1
√34	5, 1, 4, 1, 10, 1, 4, 1, 10 etc. 1 9 2 9 1 9 2 9 1
√35	5, 1, 10, 1, 10, 1, 10 etc. 1 10 1 10 1 10 1
√37	6, 12, 12, 12 etc. 1 1 1 1
√38	6, 6, 12, 6, 12, 6, 12 etc. 1 2 1 2 1 2 1
√39	6, 4, 12, 4, 12, 4, 12 etc. 1 3 1 3 1 3 1
√40	6, 3, 12, 3, 12, 3, 12 etc. 1 4 1 4 1 4 1
√41	6, 2, 2, 12, 2, 2, 12 etc. 1 5 5 1 5 5 1
√42	6, 2, 12, 2, 12, 2, 12 etc. 1 6 1 6 1 6 1
√43	6, 1, 1, 3, 1, 5, 1, 3, 1, 1, 12 etc. 1 7 6 3 9 2 9 3 6 7 1
√44	6, 1, 1, 1, 2, 1, 1, 1, 12 etc. 1 8 5 7 4 7 5 8 1
√45	6, 1, 2, 2, 2, 1, 12, 1, 2, 2, 2, 1, 12 etc. 1 9 4 5 4 9 1 9 4 5 4 9 1
√46	6, 1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12 etc. 1 10 3 7 6 5 2 5 6 7 3 10 1
√47	6, 1, 5, 1, 12, 1, 5, 1, 12 etc. 1 11 2 11 1 11 2 11 1
√48	6, 1, 12, 1, 12, 1, 12 etc. 1 12 1 12 1 12 1
√50	7, 14, 14, 14 etc. 1 1 1 1
√51	7, 7, 14, 7, 14, 7, 14 etc. 1 2 1 2 1 2 1

Numeri surdi	Indices
√52	7, 4, 1, 2, 1, 4, 14, 4, 1, 2, 1, 4, 14 etc. 1 3 9 4 9 3 1 3 9 4 9 3 1
√53	7, 3, 1, 1, 3, 14, 3, 1, 1, 3, 14 etc. 1 4 7 7 4 1 4 7 7 4 1
√54	7, 2, 1, 6, 1, 2, 14, 2, 1, 6, 1, 2, 14 etc. 1 5 9 2 9 5 1 5 9 2 9 5 1
√55	7, 2, 2, 2, 14, 2, 2, 2, 14, 2, 2, 2, 14 etc. 1 6 5 6 1 6 5 6 1 6 5 6 1
√56	7, 2, 14, 2, 14, 2, 14 etc. 1 7 1 7 1 7 1
√57	7, 1, 1, 4, 1, 1, 14 etc. 1 8 7 3 7 8 1
√58	7, 1, 1, 1, 1, 1, 1, 14 etc. 1 9 6 7 7 6 9 1
√59	7, 1, 2, 7, 2, 1, 14 etc. 1 10 5 2 5 10 1
√60	7, 1, 2, 1, 14 etc. 1 11 4 11 1
√61	7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14 etc. 1 12 3 4 9 5 5 9 4 3 12 1
√62	7, 1, 6, 1, 14 etc. 1 13 2 13 1
√63	7, 1, 14, 1, 14 etc. 1 14 1 14 1
√65	8, 16, 16 etc. 1 1 1
√66	8, 8, 16, 8, 16 etc. 1 2 1 2 1
√67	8, 5, 2, 1, 1, 7, 1, 1, 2, 5, 16 etc. 1 3 6 7 9 2 9 7 6 3 1
√68	8, 4, 16, 4, 16 etc. 1 4 1 4 1
√69	8, 3, 3, 1, 4, 1, 3, 3, 16 etc. 1 5 4 11 3 11 4 5 1
√70	8, 2, 1, 2, 1, 2, 16 etc. 1 6 9 5 9 6 1
√71	8, 2, 2, 1, 7, 1, 2, 2, 16 etc. 1 7 5 11 2 11 5 7 1
√72	8, 2, 16, 2, 16 etc. 1 8 1 8 1
√73	8, 1, 1, 5, 5, 1, 1, 16 etc. 1 9 8 3 3 8 9 1
√74	8, 1, 1, 1, 1, 16 etc. 1 10 7 7 10 1

Numeri surdi	Indices	Numeri surdi	Indices
$\sqrt{75}$	8, 1, 1, 1, 16 etc. 1 11 6 11 1	$\sqrt{98}$	9, 1, 8, 1, 18 etc. 1 17 2 17 1
$\sqrt{76}$	8, 1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16 etc. 1 12 5 8 9 3 4 3 9 8 5 12 1	$\sqrt{99}$	9, 1, 18, 1, 18 etc. 1 18 1 18 1
$\sqrt{77}$	8, 1, 3, 2, 3, 1, 16 etc. 1 13 4 7 4 13 1	$\sqrt{101}$	10, 20, 20 etc. 1 1 1
$\sqrt{78}$	8, 1, 4, 1, 16 etc. 1 14 3 14 1	$\sqrt{102}$	10, 10, 20, 10, 20 etc. 1 2 1 2 1
$\sqrt{79}$	8, 1, 7, 1, 16 etc. 1 15 2 15 1	$\sqrt{103}$	10, 6, 1, 2, 1, 1, 9, 1, 1, 2, 1, 6, 20 etc. 1 3 13 6 9 11 2 11 9 6 13 3 1
$\sqrt{80}$	8, 1, 16, 1, 16 etc. 1 16 1 16 1	$\sqrt{104}$	10, 5, 20, 5, 20 etc. 1 4 1 4 1
$\sqrt{82}$	9, 18, 18, 18 etc. 1 1 1 1	$\sqrt{105}$	10, 4, 20, 4, 20 etc. 1 5 1 5 1
$\sqrt{83}$	9, 9, 18, 9, 18 etc. 1 2 1 2 1	$\sqrt{106}$	10, 3, 2, 1, 1, 1, 1, 2, 3, 20 etc. 1 6 7 10 9 9 10 7 6 1
$\sqrt{84}$	9, 6, 18, 6, 18 etc. 1 3 1 3 1	$\sqrt{107}$	10, 2, 1, 9, 1, 2, 20 etc. 1 7 13 2 13 7 1
$\sqrt{85}$	9, 4, 1, 1, 4, 18 etc. 1 4 9 9 4 1	$\sqrt{108}$	10, 2, 1, 1, 4, 1, 1, 2, 20 etc. 1 8 9 11 4 11 9 8 1
$\sqrt{86}$	9, 3, 1, 1, 1, 8, 1, 1, 1, 3, 18 etc. 1 5 10 7 11 2 11 7 10 5 1	$\sqrt{109}$	10, 2, 3, 1, 2, 4, 1, 6, 6, 1, 4, 2, 1, 3, 2, 20 etc. 1 9 5 12 7 4 15 3 3 15 4 7 12 5 9 1
$\sqrt{87}$	9, 3, 18, 3, 18 etc. 1 6 1 6 1	$\sqrt{110}$	10, 2, 20, 2, 20 etc. 1 10 1 10 1
$\sqrt{88}$	9, 2, 1, 1, 1, 2, 18 etc. 1 7 9 8 9 7 1	$\sqrt{111}$	10, 1, 1, 6, 1, 1, 20 etc. 1 11 10 3 10 11 1
$\sqrt{89}$	9, 2, 3, 3, 2, 18 etc. 1 8 5 5 8 1	$\sqrt{112}$	10, 1, 1, 2, 1, 1, 20 etc. 1 12 9 7 9 12 1
$\sqrt{90}$	9, 2, 18, 2, 18 etc. 1 9 1 9 1	$\sqrt{113}$	10, 1, 1, 1, 2, 2, 1, 1, 1, 20 etc. 1 13 8 11 7 7 11 8 13 1
$\sqrt{91}$	9, 1, 1, 5, 1, 5, 1, 1, 18 etc. 1 10 9 3 14 3 9 10 1	$\sqrt{114}$	10, 1, 2, 10, 2, 1, 20 etc. 1 14 7 2 7 14 1
$\sqrt{92}$	9, 1, 1, 2, 4, 2, 1, 1, 18 etc. 1 11 8 7 4 7 8 11 1	$\sqrt{115}$	10, 1, 2, 1, 1, 1, 1, 1, 2, 1, 20 etc. 1 15 6 11 9 10 9 11 6 15 1
$\sqrt{93}$	9, 1, 1, 1, 4, 6, 4, 1, 1, 1, 18 etc. 1 12 7 11 4 3 4 11 7 12 1	$\sqrt{116}$	10, 1, 3, 2, 1, 4, 1, 2, 3, 1, 20 etc. 1 16 5 7 13 4 13 7 5 16 1
$\sqrt{94}$	9, 1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18, etc. 1 13 6 5 9 10 3 15 2 15 3 10 9 5 6 13 1	$\sqrt{117}$	10, 1, 4, 2, 4, 1, 20 etc. 1 17 4 9 4 17 1
$\sqrt{95}$	9, 1, 2, 1, 18 etc. 1 14 5 14 1	$\sqrt{118}$	10, 1, 6, 3, 2, 10, 2, 3, 6, 1, 20 etc. 1 18 3 6 9 2 9 6 3 18 1
$\sqrt{96}$	9, 1, 3, 1, 18 etc. 1 15 4 15 1	$\sqrt{119}$	10, 1, 9, 1, 20 etc. 1 19 2 19 1
$\sqrt{97}$	9, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18 etc. 1 16 3 11 8 9 9 8 11 3 16 1	$\sqrt{120}$	10, 1, 20, 1, 20 etc. 1 20 1 20 1

16. In omnibus his indicum seriebus periodi deprehenduntur modo strictiores modo largiores, quae indicibus iis, qui primo duplo sunt majores, includuntur, atque hae periodi eo clarius in oculos incidunt, si primi indices cujusque seriei duplicantur. Deinde in qualibet periodo idem indicum ordo, sive antrorsum, sive retrorsum, observatur: ex quo in qualibet periodo vel unus datur index medius, vel duo, prout terminorum numerus fuerit par, vel impar. In litteris vero etiam graecis similes periodi observantur, ubi imprimis animadvertendum, pro omnibus indicibus $2v$ litteram graecam in unitatem abire. Hanc proprietatem insignem, quae in ipsis operationibus facilius perspicitur, quam verborum ambage demonstratur, probe notasse in sequentibus plurimum intererit.

17. Ex his autem exemplis formas quasdam generales colligere licet, quae ita se habent:

I. Si $z = nn + 1$, erunt indices $\underset{1}{n},\ \underset{1}{2n},\ \underset{1}{2n},\ \underset{1}{2n}$ etc.

II. Si $z = nn + 2$, erunt indices $\underset{1}{n},\ \underset{2}{n},\ \underset{1}{2n},\ \underset{2}{n},\ \underset{1}{2n}$ etc.

III. Si $z = nn + n$, erunt indices $\underset{1}{n},\ \underset{n}{2},\ \underset{1}{2n},\ \underset{n}{2},\ \underset{1}{2n}$ etc.

IV. Si $z = nn + 2n - 1$, erunt indices $\underset{1}{n},\ \underset{2n-1}{1},\ \underset{2}{n-1},\ \underset{2n-1}{1},\ \underset{1}{2n}$ etc.

V. Si $z = nn + 2n$ erunt indices $\underset{1}{n},\ \underset{2n}{1},\ \underset{1}{2n},\ \underset{2n}{1},\ \underset{1}{2n}$ etc.

Ac fractionum quidem continuarum ex his indicibus formatarum valor in genere facile definitur, idemque, quem hic assignavimus, deprehenditur. Tum vero etiam patet

VI. Si sit $z = 4nn + 4$, fore indices $\underset{1}{2n},\ \underset{4}{n},\ \underset{1}{4n},\ \underset{4}{n},\ \underset{1}{4n}$ etc.

VII. Si sit $z = 9nn + 3$, fore indices $\underset{1}{3n},\ \underset{3}{2n},\ \underset{1}{6n},\ \underset{3}{2n},\ \underset{1}{6n}$ etc.

VIII. Si sit $z = 9nn + 6$, fore indices $\underset{1}{3n},\ \underset{6}{n},\ \underset{1}{6n},\ \underset{6}{n},\ \underset{1}{6n}$ etc.

De resolutione formulae $p = \sqrt{(lqq + 1)}$ in numeris integris.

18. Inventis indicibus pro radice quadrata numeri cujusvis z, ea hoc modo per fractionem continuam exprimitur:

$$\sqrt{z} = v + \cfrac{1}{a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \text{etc.}}}}}$$

atque ex his indicibus v, a, b, c, d, etc. fractiones $\frac{x}{y}$ formari possunt, quae tam prope ad $\sqrt{z}$ accedunt, ut nonnisi majoribus numeris adhibendis, ejus valor accuratius exhiberi possit. Hae fractiones autem ita formantur:

Indices $\nu, \quad a, \quad b, \quad c, \quad \ldots . m, \quad n,$

$$\frac{x}{y} \quad \frac{1}{0}, \frac{\nu}{1}, \frac{a\nu+1}{a}, \frac{(ab+1)\nu+b}{ab+1} \ldots \ldots \frac{M}{P}, \frac{N}{Q}, \frac{nN+M}{nQ+P},$$

quae continuo propius valorem irrationalem $\sqrt{z}$ exprimunt.

19. **Novus autem algorithmus succinctum modum suppeditat, has fractiones commode per indices repraesentandi, quae ita se habent:**

$$\frac{1}{0}, \frac{(\nu)}{1}, \frac{(\nu, a)}{(a)}, \frac{(\nu, a, b)}{(a, b)}, \frac{(\nu, a, b, c)}{(a, b, c)}, \frac{(\nu, a, b, c, d)}{(a, b, c, d)} \text{ etc.}$$

ubi cum ex natura progressionis sit:

$$(\nu, a) = a(\nu) + 1, \quad (\nu, a, b) = b(\nu, a) + (\nu); \quad (\nu, a, b, c) = c(\nu, a, b) + (\nu, a);$$
$$(a) = a\,1 + 0; \quad (a, b) = b(a) + 1; \quad (a, b, c) = c(a, b) + (a);$$

erit etiam ex natura harum formularum:

$$(\nu, a) = \nu(a) + 1; \quad (\nu, a, b) = \nu(a, b) + b; \quad (\nu, a, b, c) = \nu(a, b, c) + (b, c)$$

deinde etiam sequentes transformationes demonstravi:

$$(\nu, a, b, c, d, e) = \nu(a, b, c, d, e) + (b, c, d, e)$$
$$(\nu, a, b, c, d, e) = (\nu, a)(b, c, d, e) + \nu(c, d, e)$$
$$(\nu, a, b, c, d, e) = (\nu, a, b)(c, d, e) + (\nu, a)(d, e)$$
$$(\nu, a, b, c, d, e) = (\nu, a, b, c)(d, e) + (\nu, a, b)(e),$$

quas probe notasse in sequentibus plurimum juvabit.

20. Videamus jam, quam prope singulae istae fractiones ad valorem $\sqrt{z}$ accedant, quod pro instituto nostro luculentissime inde patebit, si ex quaque fractione $\frac{x}{y}$ valorem $xx - zyy$ colligamus, quippe qui quo minor fuerit prae ipsis numeris x et y, eo exactius fractio $\frac{x}{y}$ valori $\sqrt{z}$ aequabitur. Ac primo quidem si $\frac{x}{y} = \frac{1}{0}$, erit $xx - zyy = 1$. Deinde sumto $\frac{x}{y} = \frac{\nu}{1}$, fit $xx - zyy = \nu\nu - z$, quae differentia per operationes supra expositas (12) prima littera graeca negative sumta $-\alpha$ designatur. Porro posito $\frac{x}{y} = \frac{(\nu, a)}{(a)} = \frac{\nu a+1}{a}$, colligitur

$$xx - zyy = (\nu\nu - z)aa + 2\nu a + 1 = -\alpha aa + 2\nu a + 1,$$

ergo $\qquad xx - zyy = 1 + a(2\nu - \alpha a) = 1 + a(A - B) = \beta$

ob $\qquad \nu = A \quad \text{et} \quad \alpha a = A + B.$

Quocirca hoc casu fit $xx - zyy = \beta$.

21. Cum igitur nacti simus:

$$\nu\nu - z = -\alpha \quad \text{et} \quad (\nu, a)^2 - z(a)^2 = \beta$$

hinc ulterius progredi poterimus. Sit igitur

$$\frac{x}{y} = \frac{(\nu, a, b)}{(a, b)} = \frac{b(\nu, a) + \nu}{b(a) + 1}$$

atque adhibitis illis reductionibus obtinebimus

$$xx - zyy = \beta bb + 2\nu b(\nu, a) - 2zb(a) - \alpha,$$

ergo ob $(\nu, a) = \nu(a) + 1$, erit

$$xx - zyy = \beta bb - 2\alpha ab + 2\nu b - \alpha = -\alpha - b(2\alpha a - \beta b - 2\nu)$$

at est $\nu = A$, $\alpha a = A + B$ et $\beta b = B + C$, ideoque $xx - zyy = -\alpha - b(B - C) = -\gamma$, ita ut sit $(\nu, a, b)^2 - z(a, b)^2 = -\gamma$.

22. Consideremus nunc fractionem sequentem:

$$\frac{x}{y} = \frac{(\nu, a, b, c)}{(a, b, c)} = \frac{c(\nu, a, b) + (\nu, a)}{c(a, b) + a},$$

ex qua colligitur:

$$xx - zyy = -\gamma cc + 2c(\nu, a, b)(\nu, a) - 2zca(a, b) + \beta,$$

cujus pars media reducitur ad

$$2c(\beta b - \alpha a + \nu),$$

unde ob

$$\nu = A, \quad \alpha a = A + B, \quad \beta b = B + C, \quad \gamma c = C + D,$$

resultat

$$xx - zyy = \beta + c(C - D) = \delta,$$

ita ut sit $(\nu, a, b, c)^2 - z(a, b, c)^2 = \delta$, unde per inductionem sequentes valores facile colliguntur.

23. Ne autem hic inductioni nimium videar tribuisse, sequenti modo haec investigatio institui potest:

$$\begin{array}{lll}
\text{sit } (\nu)^2 & - z\,1^2 & = \mathfrak{A} \\
(\nu, a)^2 & - z(a)^2 & = \mathfrak{B} \\
(\nu, a, b)^2 & - z(a, b)^2 & = \mathfrak{C} \\
(\nu, a, b, c)^2 & - z(a, b, c)^2 & = \mathfrak{D} \\
(\nu, a, b, c, d)^2 & - z(a, b, c, d)^2 & = \mathfrak{E} \\
& \text{etc.} &
\end{array}$$

ubi quidem jam vidimus esse $\mathfrak{A} = -\alpha$, $\mathfrak{B} = \beta$, $\mathfrak{C} = -\gamma$ etc. Cum vero sit

$$\begin{array}{llll}
(\nu, a) & = a(\nu) + 1; & (a) & = a \\
(\nu, a, b) & = b(\nu, a) + (\nu); & (a, b) & = b(a) + 1 \\
(\nu, a, b, c) & = c(\nu, a, b) + (\nu, a); & (a, b, c) & = c(a, b) + (a) \\
(\nu, a, b, c, d) & = d(\nu, a, b, c) + (\nu, a, b); & (a, b, c, d) & = d(a, b, c) + (a, b) \\
& \text{etc.} & &
\end{array}$$

habebimus:

$$\begin{aligned}
\mathfrak{B} &= \mathfrak{A}aa + 1 + 2a(\nu) \\
\mathfrak{C} &= \mathfrak{B}bb + \mathfrak{A} + 2b((\nu, a)(\nu) - z(a)) \\
\mathfrak{D} &= \mathfrak{C}cc + \mathfrak{B} + 2c((\nu, a, b)(\nu, a) - z(a, b)(a)) \\
\mathfrak{E} &= \mathfrak{D}dd + \mathfrak{C} + 2d((\nu, a, b, c)(\nu, a, b) - z(a, b, c)(a, b)) \\
\mathfrak{F} &= \mathfrak{E}ee + \mathfrak{D} + 2e((\nu, a, b, c, d)(\nu, a, b, c) - z(a, b, c, d)(a, b, c)) \\
& \text{etc.}
\end{aligned}$$

24. Statuamus jam brevitatis gratia:

$$\begin{aligned}\mathfrak{B} &= 1 + \mathfrak{A}aa + 2a.O\\ \mathfrak{C} &= \mathfrak{A} + \mathfrak{B}bb + 2b.P\\ \mathfrak{D} &= \mathfrak{B} + \mathfrak{C}cc + 2c.Q\\ \mathfrak{E} &= \mathfrak{C} + \mathfrak{D}dd + 2d.R\\ \mathfrak{F} &= \mathfrak{D} + \mathfrak{E}ee + 2e.S\\ &\text{etc.}\end{aligned}$$

et ex superioribus reductionibus colligemus:

$$\begin{aligned}P - O &= a(v)^2 - az = \mathfrak{A}a\\ Q - P &= b(v, a)^2 - bz(a)^2 = \mathfrak{B}b\\ R - Q &= c(v, a, b)^2 - cz(a, b)^2 = \mathfrak{C}c\\ S - R &= d(v, a, b, c)^2 - dz(a, b, c)^2 = \mathfrak{D}d\\ &\text{etc.}\end{aligned}$$

sicque fiet

$$\begin{aligned}O &= v\\ P &= v + \mathfrak{A}a\\ Q &= v + \mathfrak{A}a + \mathfrak{B}b\\ R &= v + \mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c\\ S &= v + \mathfrak{A}a + \mathfrak{B}b + \mathfrak{C}c + \mathfrak{D}d\\ &\text{etc.}\end{aligned}$$

25. Formulae autem supra usurpatae praebent

$$\begin{aligned}A &= v\\ B &= - v + \alpha a\\ C &= v - \alpha a + \beta b\\ D &= - v + \alpha a - \beta b + \gamma c\\ E &= v - \alpha a + \beta b - \gamma c + \delta d\end{aligned}$$

unde patet esse $O = A$ et $P = -B$ ob $\mathfrak{A} = -\alpha$. Cum jam sit

$$\mathfrak{B} = 1 - \alpha aa + 2av = 1 + a(A - B),$$

erit utique $\mathfrak{B} = \beta$, hincque $Q = C$, ex quo porro colligitur:

$$\mathfrak{C} = -\alpha + \beta bb - 2bB = -\alpha - b(2B - \beta b) = -\alpha - b(B - C)$$

sicque est $\mathfrak{C} = -\gamma$ et $R = -D$; simili modo

$$\mathfrak{D} = \beta - \gamma cc + 2cC = \beta + c(2C - \gamma c) = \beta + c(C - D),$$

ideoque est $\mathfrak{D} = \delta$ et $S = E$. Tum vero porro

$$\mathfrak{E} = -\gamma + \delta dd - 2dD = -\gamma - d(2D - \delta d) = \gamma - d(D - E)$$

ac propterea $\mathfrak{E} = -\varepsilon$, unde superior inductio satis confirmatur.

26. Pro fractionibus ergo $\frac{x}{y}$ formulae radicali $\sqrt{z}$ proxime aequalibus sequentes adipiscimur relationes:

Si sumatur

$$\begin{cases} x = 1 \\ y = 0 \end{cases} \text{ erit } xx = zyy + 1$$

$$\begin{cases} x = (v) \\ y = (1) \end{cases} \text{ erit } xx = zyy - \alpha$$

$$\begin{cases} x = (v, a) \\ y = (a) \end{cases} \text{ erit } xx = zyy + \beta$$

$$\begin{cases} x = (v, a, b) \\ y = (a, b) \end{cases} \text{ erit } xx = zyy - \gamma$$

$$\begin{cases} x = (v, a, b, c) \\ y = (a, b, c) \end{cases} \text{ erit } xx = zyy + \delta$$

$$\begin{cases} x = (v, a, b, c, d) \\ y = (a, b, c, d) \end{cases} \text{ erit } xx = zyy - \varepsilon$$

etc.

unde problema Pellianum solvetur, quoties litterarum graecarum per saltum excerptarum β, δ, ζ etc. quaepiam in unitatem abit.

27. Vidimus autem supra, nonnisi iis indicibus, qui sunt $2v$, respondere litteram graecam in unitatem abeuntem; cum igitur quaelibet periodorum, quas in indicum ordine observavimus, indice $2v$ inchoetur, perspicuum est, si numeros x et y per indices primae periodi definiamus, fore vel $xx = zyy - 1$, vel $xx = zyy + 1$; ac prius quidem evenit, si indicum singulas periodos constituentium numerus fuerit impar, posterius vero si is fuerit par. Hoc igitur casu statim habetur solutio problematis Pelliani, quo requiritur, ut sit $pp = zqq + 1$, quandoquidem capi oportet $p = x$ et $q = y$.

28. At si ex prima periodo prodeat $xx = zyy - 1$, quod evenit si indicum numerus est impar, tum indices usque ad initium tertiae periodi ad definiendos numeros x et y capi possent, quorum numerus cum sit par, hoc modo idonei numeri pro p et q obtinerentur. Verum casu invento, quo fit $xx = zyy - 1$, multo facilius inde numeri p et q reperiri possunt, ut sit: $pp = zqq + 1$. Sumatur enim $p = 2xx + 1$ et $q = 2xy$, eritque

$$pp - zqq = 4x^4 + 4xx + 1 - 4zxxyy = 1 + 4xx(xx - zyy + 1),$$

at $xx - zyy + 1 = 0$, ideoque $pp - zqq = 1$, seu $pp = zqq + 1$, quemadmodum problema Pellianum postulat. Videamus igitur, quomodo pro quovis numero z ex indicibus inde natis numeri p et q sint definiendi, ut fiat $pp = zqq + 1$, ubi quidem casus secundum periodos percurramus.

I. Casus, quo pro numero z indices sunt v, $2v$, $2v$, etc.

29. Hic singulae periodi unicum indicem continent, sumto ergo $x = (v)$ et $y = 1$, erit $xx = zyy - 1$. Quamobrem, ut fiat $pp = zqq + 1$, capiatur:

$$p = 2xx + 1 = 2vv + 1 \quad \text{et} \quad q = 2xy = 2v.$$

Hic casus, ut supra vidimus, locum habet, si sit $z = vv + 1$, seu quo numerus z unitate superat quadratum; tum igitur capi debet $p = 2vv + 1$, seu $p = 2z - 1$ et $q = 2v$, quo pacto problemati Pelliano satisfit, ut sit $p = \sqrt{(zqq + 1)}$. Ita si sit

$z = 2$, erit $p = 3$ et $q = 2$, sicque $p = \sqrt{(2qq + 1)}$;
si $z = 5$, erit $p = 9$ et $q = 4$, sicque $p = \sqrt{(5qq + 1)}$;
si $z = 10$, erit $p = 19$ et $q = 6$, sicque $p = \sqrt{(10qq + 1)}$;
si $z = 17$, erit $p = 33$ et $q = 8$, sicque $p = \sqrt{(17qq + 1)}$;
etc.

II. Casus, quo pro numero z indices sunt $v, a, 2v, a, 2v$ etc.

30. Prima periodus constat binis numeris v, a, unde sumtis $x = (v, a) = va + 1$ et $y = (a) = a$, habebitur $xx = zyy + 1$. Ut igitur pro problemate Pelliano fiat $pp = zqq + 1$, capi oportet:

$$p = va + 1 \quad \text{et} \quad q = a.$$

Ex indicibus autem patet, hunc casum locum habere, quoties fuerit numerus $z = vv + \frac{2v}{a}$, unde intelligitur, hunc casum in integris, de quibus hic agitur, existere non posse, nisi sit a divisor ipsius $2v$, ubi duo casus sunt considerandi:

1. si $a = 2n$, erit $v = mn$ et $\frac{2v}{a} = m$,

2. si $a = 2n + 1$, erit $v = m(2n + 1)$ et $\frac{2v}{a} = 2m$.

III. Casus, quo pro numero z indices sunt $v, a, a, 2v, a, a, 2v$ etc.

31. Ex prima periodo, sumtis numeris x et y, ita ut sit $x = (v, a, a)$ et $y = (a, a)$, erit $xx = zyy - 1$; unde ut fiat $pp = zqq + 1$, sumi debet

$$p = 2xx + 1 \quad \text{et} \quad q = 2xy.$$

Hic vero est $y = aa + 1$ et $x = vy + a$, unde numeri p et q facillime definiuntur. Ex indicibus autem numerus z ejusmodi habebit formam:

$$z = vv + u, \quad \text{existente} \quad u = \frac{2av + 1}{aa + 1},$$

unde patet numerum a esse debere parem. Si ergo statuatur $a = 2n$, necesse est sit

$$v = n + m(4nn + 1), \quad \text{tumque fit} \quad u = 1 + 4mn.$$

IV. Casus, quo pro numero z indices sunt $v, a, b, a, 2v, a, b, a, 2v$ etc.

32. Quia numerus indicum in quaque periodo est par, si sumatur:

$$x = (v, a, b, a) \quad \text{et} \quad y = (a, b, a),$$

$$\text{erit} \quad xx = zyy + 1, \quad \text{ideoque} \quad p = x \quad \text{et} \quad q = y.$$

Per transformationes autem supra ostensas duplicatio indicum tolli potest hoc modo:

$$x = (a)(\nu, a.\,b) + (\nu, a) \quad \text{et} \quad y = (a)(a, b) + (a).$$

Hinc si ex indicibus ν, a, b sequentes fractiones formentur:

$$\begin{array}{llll} \text{indices} & \nu, & a, & b \\ \text{fractiones} & \frac{1}{0}, & \frac{\mathfrak{A}}{\mathfrak{a}}, & \frac{\mathfrak{B}}{\mathfrak{b}}, \ \frac{\mathfrak{C}}{\mathfrak{c}}, \end{array}$$

$$\text{ob} \quad \mathfrak{A} = (\nu), \quad \mathfrak{B} = (\nu, a), \quad \mathfrak{C} = (\nu, a, b)$$

$$\text{et} \quad \mathfrak{a} = 1, \quad \mathfrak{b} = (a), \quad \mathfrak{c} = (a, b),$$

$$\text{erit} \quad x = \mathfrak{b}\mathfrak{C} + \mathfrak{a}\mathfrak{B} \quad \text{et} \quad y = \mathfrak{b}\mathfrak{c} + \mathfrak{a}\mathfrak{b}.$$

Ex indicibus autem fit $z = \nu\nu + u$, existente

$$2\nu = m(a, b, a) - b(a, b)$$

$$\text{et} \quad u = m(a, b) - b(b).$$

V. Casus, quo pro numero z indices sunt ν, a, b, b, a, 2ν etc.

33. Ob indicum cujusque periodi numerum imparem, si capiamus

$$x = (\nu, a, b, b, a) \quad \text{et} \quad y = (a, b, b, a),$$

erit $xx = zyy - 1$; hinc pro problemate Pelliano, ut fiat $pp = zqq + 1$, statui oportet:

$$p = 2xx + 1 \quad \text{et} \quad q = 2xy.$$

Quo autem numeri x et y facilius inveniri queant, sequentes transformationes instituantur:

$$x = (a, b)(\nu, a, b) + (a)(\nu, a) \quad \text{et} \quad y = (a, b)(a, b) + (a)(a),$$

qui ergo per solos indices ν, a, b fractionibus inde formandis definientur:

$$\begin{array}{llll} \text{indices} & \nu, & a, & b \\ \text{fractiones} & \frac{1}{0}, & \frac{\mathfrak{A}}{\mathfrak{a}}, & \frac{\mathfrak{B}}{\mathfrak{b}}, \ \frac{\mathfrak{C}}{\mathfrak{c}}, \end{array}$$

$$\text{ubi} \quad \mathfrak{A} = \nu, \mathfrak{B} = a\mathfrak{A} + 1, \quad \mathfrak{C} = b\mathfrak{B} + \mathfrak{A}$$

$$\text{et} \quad \mathfrak{a} = 1, \ \mathfrak{b} = a\mathfrak{a} + 0, \quad \mathfrak{c} = b\mathfrak{b} + \mathfrak{a};$$

tum enim capi oportet

$$x = \mathfrak{c}\mathfrak{C} + \mathfrak{b}\mathfrak{B} \quad \text{et} \quad y = \mathfrak{c}\mathfrak{c} + \mathfrak{b}\mathfrak{b}.$$

Hic autem casus locum habet, quoties posito $z = \nu\nu + u$ fuerit

$$2\nu = m(a, b, b, a) + (b, b)(a, b, b) \quad \text{et} \quad u = m(a, b, b) + (b, b)(b, b).$$

VI. Casus, quo pro numero z indices sunt ν, a, b, c, b, a, 2ν etc.

34. Quoniam hic numerus indicum in qualibet periodo est par, si sumamus

$$x = (\nu, a, b, c, b, a) \quad \text{et} \quad y = (a, b, c, b, a),$$

erit $xx = zyy + 1$, ideoque pro Pelliano problemate statim habetur $p = x$ et $q = y$. Facilius autem numeri x et y his transformationibus adhibitis invenientur:

$$x = (a, b)(\nu, a, b, c) + (a)(\nu, a, b) \quad \text{et} \quad y = (a, b)(a, b, c) + (a)(a, b),$$

unde si ex indicibus v, a, b, c, more exposito, fractiones formentur:

$$\begin{array}{llllll} \text{indices} & v, & a, & b, & c & \\ \text{fractiones} & \frac{1}{0}, & \frac{\mathfrak{A}}{\mathfrak{a}}, & \frac{\mathfrak{B}}{\mathfrak{b}}, & \frac{\mathfrak{C}}{\mathfrak{c}}, & \frac{\mathfrak{D}}{\mathfrak{d}}, \end{array}$$

sumi oportet

$$x = \mathfrak{c}\mathfrak{D} + \mathfrak{d}\mathfrak{C} \quad \text{et} \quad y = \mathfrak{c}\mathfrak{d} + \mathfrak{d}\mathfrak{c}.$$

At hic casus locum habet, quoties posito $z = vv + u$ fuerit

$$2v = m(a, b, c, b, a) - (b, c, b)(a, b, c, b) \quad \text{et} \quad u = m(a, b, c, b) - (b, c, b)(b, c, b).$$

VII. Casus, quo pro numero z indices sunt v, a, b, c, c, b, a, $2v$ etc.

35. Hic iterum indicum numerus in qualibet periodo est impar, ideoque si ponamus

$$x = (v, a, b, c, c, b, a) \quad \text{et} \quad y = (a, b, c, c, b, a),$$

erit $xx = zyy - 1$, ex quo ut fiat $pp = zqq + 1$, sumi oportet $p = 2xx + 1$, et $q = 2xy$. Pro faciliori autem numerorum x et y inventione ex indicibus v, a, b, c formentur fractiones:

$$\begin{array}{llllll} \text{indices} & v, & a, & b, & c & \\ \text{fractiones} & \frac{1}{0}, & \frac{\mathfrak{A}}{\mathfrak{a}}, & \frac{\mathfrak{B}}{\mathfrak{b}}, & \frac{\mathfrak{C}}{\mathfrak{c}}, & \frac{\mathfrak{D}}{\mathfrak{d}}, \end{array}$$

hincque erit

$$x = \mathfrak{d}\mathfrak{D} + \mathfrak{c}\mathfrak{C} \quad \text{et} \quad y = \mathfrak{d}\mathfrak{d} + \mathfrak{c}\mathfrak{c}.$$

At hic casus locum habebit, quoties posito $z = vv + u$ fuerit:

$$2v = m(a, b, c, c, b, a) + (b, c, c, b)(a, b, c, c, b) \quad \text{et} \quad u = m(a, b, c, c, b) + (b, c, c, b)(b, c, c, b).$$

VIII. Casus, quo pro numero z indices sunt v, a, b, c, d, c, b, a, $2v$ etc.

36. Hic quaelibet periodus octo continet indices; ideoque si ponamus:

$$x = (v, a, b, c, d, c, b, a) \quad \text{et} \quad y = (a, b, c, d, c, b, a),$$

erit $xx = zyy + 1$, et pro problemate Pelliano capi oportet $p = x$ et $q = y$, ut fiat $pp = zqq + 1$. Transformationibus autem adhibitis, numeros x et y per solos indices v, a, b, c, d definire licet. Formatis enim inde fractionibus:

$$\begin{array}{lllllll} \text{indices} & v, & a, & b, & c, & d & \\ \text{fractiones} & \frac{1}{0}, & \frac{\mathfrak{A}}{\mathfrak{a}}, & \frac{\mathfrak{B}}{\mathfrak{b}}, & \frac{\mathfrak{C}}{\mathfrak{c}}, & \frac{\mathfrak{D}}{\mathfrak{d}}, & \frac{\mathfrak{E}}{\mathfrak{e}}, \end{array}$$

fiet: $x = \mathfrak{d}\mathfrak{E} + \mathfrak{c}\mathfrak{D}$ et $y = \mathfrak{d}\mathfrak{e} + \mathfrak{c}\mathfrak{d}$.

Hic vero casus locum habet, quoties posito $z = vv + u$ fuerit:

$$2v = m(a, b, c, d, c, b, a) - (b, c, d, c, b)(a, b, c, d, c, b)$$
$$\text{et} \quad u = m(a, b, c, d, c, b) - (b, c, d, c, b)(b, c, d, c, b).$$

Expositio calculi pro quolibet numero z, ut fiat $pp = zqq + 1$.

37. Primum igitur methodo supra exposita pro numero z, ex ejus radice quadrata indices investigari oportet, quam operationem autem ulterius continuari non est opus, quam donec indices

ordine retrogrado prodire incipiant, quo pacto semissi laboris supra explicati supersedere poterimus. Cum autem in prima periodo vel unus index medius occurrat, vel bini, hi casus probe sunt distinguendi: cum si unicus medius affuerit, inventio numerorum p et q modo in casibus II, IV, VI et VIII tradito institui debeat; sin autem bini fuerint medii, eo modo, qui in casibus I, III, V et VII est descriptus. Scilicet si prius eveniat, numeri p et q numeris x et y aequales sumuntur; sin autem posterius, uti vidimus, statui oportet $p = 2xx + 1$, et $q = 2xy$, ita ut his casibus numeri p et q caeteris paribus multo grandiores reperiantur.

38. En igitur exempla prioris generis, quo in qualibet periodo unus datur index medius:

I. Si $z = 6$, sunt indices 2, 2, 4, hinc operatio

$$\begin{array}{cccc} & 2 & 2 & \\ \frac{1}{0}, & \frac{2}{1}, & \frac{5}{2}, \end{array} \quad \begin{array}{l} x = 1.5 + 0.2 \\ y = 1.2 + 0.1 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 5 \\ q = 2. \end{array}$$

II. Si $z = 14$, sunt indices 3, 1, 2, 1, 6

$$\begin{array}{cccc} 3 & 1 & 2 & \\ \frac{1}{0}, & \frac{3}{1}, & \frac{4}{1}, & \frac{11}{3}, \end{array} \quad \begin{array}{l} x = 1.11 + 1.4 \\ y = 1.\ 3 + 1.1 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 15 \\ q = \ 4. \end{array}$$

III. Si $z = 19$, sunt indices 4, 2, 1, 3, 1, 2, 8

$$\begin{array}{ccccc} 4 & 2 & 1 & 3 & \\ \frac{1}{0}, & \frac{4}{1}, & \frac{9}{2}, & \frac{13}{3}, & \frac{48}{11}, \end{array} \quad \begin{array}{l} x = 3.48 + 2.13 \\ y = 3.11 + 2.3 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 170 \\ q = \ 39. \end{array}$$

IV. Si $z = 31$, sunt indices 5, 1, 1, 3, 5, 3, 1, 1, 10

$$\begin{array}{cccccc} 5 & 1 & 1 & 3 & 5 & \\ \frac{1}{0}, & \frac{5}{1}, & \frac{6}{1}, & \frac{11}{2}, & \frac{39}{7}, & \frac{206}{37}, \end{array} \quad \text{hinc} \quad \begin{array}{l} x = 7.206 + 2.39 \\ y = 7.\ 37 + 2.\ 7 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 1520 \\ q = \ 273. \end{array}$$

V. Si $z = 44$, sunt indices 6, 1, 1, 1, 2, 1, 1, 1, 12

$$\begin{array}{cccccc} 6 & 1 & 1 & 1 & 2 & \\ \frac{1}{0}, & \frac{6}{1}, & \frac{7}{1}, & \frac{13}{2}, & \frac{20}{3}, & \frac{53}{8}, \end{array} \quad \text{hinc} \quad \begin{array}{l} x = 3.53 + 2.20 \\ y = 3.\ 8 + 2.\ 3 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 199 \\ q = \ 30. \end{array}$$

VI. Si $z = 55$, sunt indices 7, 2, 2, 2, 14

$$\begin{array}{cccc} 7 & 2 & 2 & \\ \frac{1}{0}, & \frac{7}{1}, & \frac{15}{2}, & \frac{37}{5}, \end{array} \quad \text{hinc} \quad \begin{array}{l} x = 2.37 + 1.15 \\ y = 2.\ 5 + 1.\ 2 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 89 \\ q = 12. \end{array}$$

39. Alterius vero generis, quo bini dantur indices medii in qualibet periodo, haec adjungo exempla:

I. Si $z = 13$, sunt indices 3, 1, 1, 1, 1, 6

$$\begin{array}{cccc} 3 & 1 & 1 & \\ \frac{1}{0}, & \frac{3}{1}, & \frac{4}{1}, & \frac{7}{2}, \end{array} \quad \text{hinc} \quad \begin{array}{l} x = 2.7 + 1.4 = 18 \\ y = 2.2 + 1.1 = \ 5 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 2xx + 1 = 649 \\ q = 2xy \quad\quad = 180. \end{array}$$

II. Si $z = 29$, sunt indices 5, 2, 1, 1, 2, 10

$$\begin{array}{cccc} 5 & 2 & 1 & \\ \frac{1}{0}, & \frac{5}{1}, & \frac{11}{2}, & \frac{16}{3}, \end{array} \quad \text{hinc} \quad \begin{array}{l} x = 3.16 + 2.11 = 70 \\ y = 3.\ 3 + 2.\ 2 = 13 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 2xx + 1 = 9801 \\ q = 2xy \quad\quad = 1820. \end{array}$$

III. Si $z = 58$, sunt indices 7, 1, 1, 1, 1, 1, 1, 14

$$\begin{array}{ccccc} 7 & 1 & 1 & 1 & \\ \frac{1}{0}, & \frac{7}{1}, & \frac{8}{1}, & \frac{15}{2}, & \frac{23}{3}, \end{array} \quad \text{hinc} \quad \begin{array}{l} x = 3.23 + 2.15 = 99 \\ y = 3.\ 3 + 2.\ 2 = 13 \end{array} \quad \text{ergo} \quad \begin{array}{l} p = 2xx + 1 = 19603 \\ q = 2xy \quad = 2574. \end{array}$$

IV. Si $z = 61$, indices sunt 7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14

$$\begin{array}{ccccccc} 7 & 1 & 4 & 3 & 1 & 2 & \\ \frac{1}{0}, & \frac{7}{1}, & \frac{8}{1}, & \frac{39}{5}, & \frac{125}{16}, & \frac{164}{21}, & \frac{453}{58}, \end{array} \quad \text{hinc fit} \quad \begin{array}{l} x = 58.453 + 21.164 = 29718 \\ y = 58.\ 58 + 21.\ 21 = 3805 \end{array}$$

$$\text{ergo} \quad \begin{array}{l} p = 2xx + 1 = 1766319049 \\ q = 2xy \quad = 226153980. \end{array}$$

40. Quodsi pro majoribus numeris z, quam ante sunt evoluti, quaeri debeant numeri p et q, ut sit $pp = zqq + 1$, primum methodo supra exposita (§ 12) indices v, a, b, c, d etc. quaeri oportet, quos autem ulterius continuari non est opus, quam donec ad indicem medium, vel binos medios primae periodi perveniatur; tum vero ex iis per operationes hic descriptas primo numeri x et y, tum vero ipsi quaesiti p et q determinabuntur. Id quod aliquibus exemplis illustrari conveniet.

I. *Quaerantur numeri* p *et* q, *ut sit* $pp = 157qq + 1$.

41. Cum hic sit $z = 157$, erit $v = 12$, et $\alpha = 13$, unde indicum inventio ita se habebit:

$$\begin{array}{lll} A = 12, & \alpha = 13, & a = 1 \\ B = 1, & \beta = 12, & b = 1 \\ C = 11, & \gamma = 3, & c = 7 \\ D = 10, & \delta = 19, & d = 1 \\ E = 9, & \varepsilon = 4, & e = 5 \\ F = 11, & \zeta = 9, & f = 2 \\ G = 7, & \eta = 12, & g = 1 \\ H = 5, & \vartheta = 11, & h = 1 \\ J = 6, & \iota = 11, & i = 1 \end{array} \left.\begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right\} \text{medii.}$$

Hinc ob binos medios exemplum ad genus secundum pertinet, et operationes ita sunt instituendae:

$$\begin{array}{cccccccccc} 12 & 1 & 1 & 7 & 1 & 5 & 2 & 1 & 1 & \\ \frac{1}{0}, & \frac{12}{1}, & \frac{13}{1}, & \frac{25}{2}, & \frac{188}{15}, & \frac{213}{17}, & \frac{1253}{100}, & \frac{2719}{217}, & \frac{3972}{317}, & \frac{6691}{534}. \end{array}$$

Hinc erit

$$x = 534.6691 + 317.3972 = 4832118$$
$$\text{et} \quad y = 534.\ 534 + 317.\ 317 = 385645.$$

Quocirca

$$p = 2xx + 1 = 46698728731849$$
$$\text{et} \quad q = 2xy \quad = 3726964292220$$

atque hi adeo sunt minimi numeri integri formulae $p = \sqrt{(157qq + 1)}$ satisfacientes.

II. *Quaerantur numeri* p *et* q, *ut sit* pp = 367 qq + 1.

42. Hinc ergo est $z = 367$, $v = 19$, hincque

$$\begin{array}{lll}
A = 19, & \alpha = 6, & a = 6 \\
B = 17, & \beta = 13, & b = 2 \\
C = 9, & \gamma = 22, & c = 1 \\
D = 13, & \delta = 9, & d = 9 \\
E = 14, & \varepsilon = 19, & e = 1 \\
F = 5, & \zeta = 18, & f = 1 \\
G = 13, & \eta = 11, & g = 2 \\
H = 9, & \vartheta = 26, & h = 1 \\
J = 17, & \iota = 3, & i = 12 \\
K = 19, & \varkappa = 2, & k = 19 \text{ medius} \\
L = 19, & \lambda = 3, & l = 12
\end{array}$$

hoc ergo exemplum ad genus primum pertinet,

$$\begin{array}{cccccccccccc}
 & 19 & 6 & 2 & 1 & 9 & 1 & 1 & 2 & 1 & 12 & 19 \\
\frac{1}{0}, & \frac{19}{1}, & \frac{115}{6}, & \frac{249}{13}, & \frac{364}{19}, & \frac{3525}{184}, & \frac{3889}{203}, & \frac{7414}{387}, & \frac{18717}{977}, & \frac{26131}{1364}, & \frac{332289}{17345}, & \frac{6339622}{330919}.
\end{array}$$

Hinc erit

$$x = 17345 . 6339622 + 1364 . 332289$$

$$\text{et} \quad y = 17345 . \ 330919 + 1364 . \ 17345,$$

ex quo minimi numeri satisfacientes sunt:

$$p = 110413985786$$

$$q = 5763448635.$$

Tabula numerorum *p* et *q*,

quibus fit *pp* = *lqq* + 1, pro omnibus valoribus numeri *l* usque ad 100.

l	*q*	*p*	*l*	*q*	*p*
2	2	3	17	8	33
3	1	2	18	4	17
5	4	9	19	39	170
6	2	5	20	2	9
7	3	8	21	12	55
8	1	3	22	42	197
10	6	19	23	5	24
11	3	10	24	1	5
12	2	7	26	10	51
13	180	649	27	5	26
14	4	15	28	24	127
15	1	4	29	1820	9801

l	q	p	l	q	p	l	q	p
30	2	11	54	66	485	77	40	351
31	273	1520	55	12	89	78	6	53
32	3	17	56	2	15	79	9	80
33	4	23	57	20	151	80	1	9
34	6	35	58	2574	19603	82	18	163
35	1	6	59	69	530	83	9	32
37	12	73	60	4	31	84	6	55
38	6	37	61	226153980	1766319049	85	30906	285769
39	4	25	62	8	63	86	1122	10405
40	3	19	63	1	8	87	3	28
41	320	2049	65	16	129	88	21	197
42	2	13	66	8	65	89	53000	500901
43	531	3482	67	5967	48842	90	2	19
44	30	199	68	4	33	91	165	1574
45	24	161	69	936	7775	92	120	1151
46	3588	24335	70	30	251	93	1260	12151
47	7	48	71	413	3480	94	221064	2143295
48	1	7	72	2	17	95	4	39
50	14	99	73	267000	2281249	96	5	49
51	7	50	74	430	3699	97	6377352	62809633
52	90	649	75	3	26	98	10	99
53	9100	33125	76	6630	57799	99	1	10

Exempla denique quaedam numerorum majorum pro l assumtorum adjungam:

si $l = 103$ erit $\begin{cases} p = 227528 \\ q = 22419 \end{cases}$

si $l = 109$ erit $\begin{cases} p = 158070671986249 \\ q = 15140424455100 \end{cases}$

$l = 113$ $\begin{cases} p = 1204353 \\ q = 113296 \end{cases}$

$l = 157$ $\begin{cases} p = 46698728731849 \\ q = 3726964292220 \end{cases}$

$l = 367$ $\begin{cases} p = 110413985786 \\ q = 5763448635. \end{cases}$

XXIV.

Solution d'une question curieuse qui ne paraît soumise à aucune analyse.

(Mémoires de Berlin 1759. p. 310.)

1. Je me trouvai un jour dans une compagnie où, à l'occasion du jeu d'échecs, quelqu'un proposa cette question: de parcourir avec un cavalier toutes les cases d'un échiquier, sans parvenir jamais deux fois à la même, et en commençant par une case donnée. On mettait, pour cette fin, des jetons sur toutes les 64 cases de l'échiquier, à l'exception de celle où le cavalier devait commencer sa route; et de chaque case, où le cavalier passait conformément à sa marche, on ôtait le jeton, de sorte qu'il s'agissait d'enlever de cette façon successivement tous les jetons. Il fallait donc éviter, d'un côté, que le cavalier ne revînt à une case vide, et d'un autre côté, il fallait diriger sa course en sorte qu'il parcourût enfin toutes les cases.

2. Ceux qui croyaient cette question assez aisée, firent plusieurs essais inutiles, sans pouvoir atteindre au but; après quoi celui qui avait proposé la question, ayant commencé par une case donnée, a su si bien diriger la route, qu'il a heureusement enlevé tous les jetons. Cependant la multitude des cases ne permettait pas qu'on ait pu imprimer à la mémoire la route qu'il avait suivie; et ce n'était qu'après plusieurs essais, que j'ai enfin rencontré une telle route qui satisfait à la question; encore ne valait-elle que pour une certaine case initiale. Je ne me souviens plus, si on lui a laissé la liberté de la choisir lui-même; mais il a très positivement assuré qu'il était en état de l'exécuter, quelle que soit la case où l'on voulut qu'il commençât.

3. Pour éclaircir mieux cette question, j'ajouterai ici une route où, en commençant par un coin de l'échiquier, on parcourt toutes les cases:

42	59	44	9	40	21	46	7
61	10	41	58	45	8	39	20
12	43	60	55	22	57	6	47
53	62	11	30	25	28	19	38
32	13	54	27	56	23	48	5
63	52	31	24	29	26	37	18
14	33	2	51	16	35	4	49
1	64	15	34	3	50	17	36

J'ai marqué ici les cases par l'ordre des nombres, suivant lequel elles sont successivement parcourues. Ainsi le cavalier ayant été posé dans la case 1, saute en 2, de là en 3, et puis en 4,

5, 6 etc. jusqu'à ce que, venant enfin dans la case 64, il aura passé par toutes les cases. Il est évident que cette route satisfait également, quand on veut commencer par l'un quelconque des autres angles.

4. En retournant par la même route, on pourra aussi commencer par la case 64, et de là, en passant successivement par les cases 63, 62, 61 etc. on parviendra enfin, après avoir parcouru toutes les cases, à celle du coin 1. Mais cette route ne servira de rien, quand on doit commencer par quelque autre case: et alors on sera obligé de chercher, par des essais, une nouvelle route dont le commencement soit dans la case donnée. Or, on reconnaîtra aisément, qu'une telle solution du problème proposé serait trop pénible, et ne conviendrait pas au but en vue, où il s'agit de trouver promptement la route qu'il faut suivre. D'ailleurs, une telle recherche ne mérite aucune attention, à moins quelle ne soit fondée sur quelques principes, ou qu'on ne la puisse soumettre à quelque espèce d'analyse qui en dirige les opérations.

5. Ce n'est aussi que dans cette vue que j'ose proposer mes recherches sur cette question, recherches auxquelles j'ai été conduit par une idée toute particulière que M. Bertrand de Genève m'a fournie; car, quoiqu'elle soit légère en elle-même et tout-à-fait étrangère à la géométrie, elle doit être regardée comme très remarquable, dès qu'on aura trouvé moyen d'y appliquer l'analyse. Or, je ferai voir qu'elle est susceptible d'une analyse toute particulière qui doit mériter d'autant plus d'attention, que cette analyse demande des raisonnements peu usités ailleurs. On convient aisément de l'excellence de l'analyse, mais on la croit communément bornée à de certaines recherches qu'on rapporte aux mathématiques, et partant il sera toujours fort important d'en faire usage dans des matières qui lui semblent refuser tout accès: puisqu'il est certain qu'elle renferme l'art de raisonner dans le plus haut degré. On ne saurait donc étendre les bornes de l'analyse, sans qu'on ait raison de s'en promettre de très grands avantages.

6. Or, d'abord je remarque qu'on pourrait satisfaire à la question, si l'on trouvait une telle route, où la dernière case marquée par 64 serait éloignée de la première 1 d'un saut de cavalier, de sorte qu'il pourrait sauter de la dernière sur la première. Car ayant trouvé une telle route rentrante en elle même, on pourra commencer par quelque case que ce soit, et de là continuer la course suivant l'ordre des nombres jusqu'à la case marquée par 64, d'où en sautant à celle qui est marquée par 1, il achèverait sa course jusqu'à retourner à celle d'où il était parti. Or, voilà une telle route rentrante en elle-même:

42	57	44	9	40	21	46	7
55	10	41	58	45	8	39	20
12	43	56	61	22	59	6	47
63	54	11	30	25	28	19	38
32	13	62	27	60	23	48	5
53	64	31	24	29	26	37	18
14	33	2	51	16	35	4	49
1	52	15	34	3	50	17	36

7. Ayant donc bien imprimé à la mémoire une telle route, on sera en état de satisfaire à la question en commençant par une case quelconque. Car, soit par ex. la case marquée par 25 celle, d'où le cavalier doit partir, et on n'aura qu'à le faire marcher successivement par les cases 26, 27, 28..... jusqu'à 64, d'où passant à la case 1, il poursuivra sa route par les cases 2, 3, 4..... jusqu'à ce qu'il soit parvenu à celle qui est marquée par 24, et ainsi il aura parcouru toutes les cases de l'échiquier. J'indiquerai cette route en représentant les nombres qui marquent les cases, en sorte

25 ..... 64.1 24,

et il est est évident qu'on réussira également en commençant par toute autre case: ainsi cette disposition

46 ..... 64.1 45

servira quand on doit commencer par la case 46.

8. Il est aussi évident que la même disposition fournit, pour chaque case où l'on doit commencer, une double route: puisqu'on peut également passer de la case marquée contre l'ordre des nombres jusqu'à celle qui contient 1, et de là, sautant en 64, continuer la course par les cases 63, 62, 61 etc. jusqu'à ce qu'on parvienne à celle où l'on a commencé. Que le nombre 40 indique la case d'où il faut partir, et on aura ces deux routes à poursuivre

40.41 ..... 64.1.2 39,

et 40.39 ..... 1.64.63 41,

où la première finit par la case 39, et l'autre par 41. Toute autre disposition rentrante en elle même fournira les mêmes avantages, et il suffit d'en savoir une seule par coeur: mais on comprendra aisément que ce serait un ouvrage extrêmement embarassant, que de trouver en tâtonnant par plusieurs essais une telle disposition, et qu'on risquerait de n'y réussir peut-être jamais.

9. Je m'en vais donc expliquer une methode certaine qui nous conduira infailliblement au but proposé, et par le moyen de laquelle on sera en état de découvrir autant de routes satisfaisantes qu'on voudra: car, quoique le nombre de ces routes ne soit pas infini, il sera toujours si grand qu'on ne le saurait jamais épuiser. Mais il faut ici distinguer deux espèces de routes, l'une qui parcourt simplement toutes les cases de l'échiquier sans que le cavalier puisse sauter de la dernière à la première; l'autre espèce est celle des routes rentrantes en elles-mêmes, où le cavalier, après avoir parcouru toutes les cases, peut sauter de la dernière à la première. J'ai donné un exemple de la première espèce dans le § 3, et un de la seconde dans le § 6. L'on peut regarder l'un et l'autre comme trouvés par hasard en tâtonnant; mais la méthode que j'expliquerai, servira à en trouver autant qu'on voudra, tant de l'une que de l'autre espèce.

10. Comme il est beaucoup plus difficile de trouver, par les seuls essais, une route de la seconde espèce, je commencerai par donner une méthode par le moyen de laquelle on pourra, après avoir trouvé une route de la première espèce, en découvrir non seulement une, mais plusieurs de la seconde espèce. Pour cet effet, je remarque d'abord qu'on peut, en plusieurs manières, changer la dernière case, celle du commencament demeurant la même. Considérons la route rapportée § 3,

et qu'on marque les cases auxquelles le cavalier pourrait passer de la dernière, marquée par 64; or on verra que ces cases sont 63, 31 et 51, dont la première, qui renferme le saut déjà employé à 64, n'est d'aucun usage. Mais, puisqu'on peut passer de la case 31 à la case 64, qu'on fasse ce saut après être parvenu de la case 1, par les cases 2, 3, 4 etc. à celle de 31, et puis, qu'on poursuive la route par les cases 64, 63, 62 etc. jusqu'à ce qu'on parvienne à la case 32 qui sera à présent la dernière: Cette nouvelle route sera représentée en sorte

1.2.....31.64.63.....32.

11. De même, le saut de 64 à 51 nous donne à connaître qu'on peut passer de la case 51 à 64: et de là, en poursuivant la route par les cases 63, 62 etc. la dernière sera celle qui est marquée par 52. Cette route entière sera donc représentée en sorte:

1.2.....51.64.63.....52.

Maintenant, puisque cette dernière case 52 fournit un saut à la première, cette route se rapporte à la seconde espèce, et est rentrante en elle-même: et c'est précisément la route décrite au § 6. Quand on ne serait pas encore parvenu à une route rentrante, on pourrait de nouveau transformer celle que nous venons de trouver au § précédent:

1.....31.64.....32

où la dernière case étant 32, le cavalier en peut sauter aux cases 43, 11, 31, 33; ainsi on n'aura qu'à renverser la partie de cette route comprise entre l'un de ces nombres et le dernier 32.

12. Le nombre 43 fournira donc cette nouvelle route

1.....31.64.....43.32.....42,

où la case angulaire 42 est la dernière. Le second nombre 11 donnera cette route:

1.....11.32.....64.31.....12,

où la case marquée de 12 est à présent la dernière. Le troisième nombre 31 rend la route principale d'où nous avons tiré ces nouvelles, savoir

1.....31.32.....64,

et le quatrième nombre 33 ne change rien dans la route que nous traitons. La route précédente, qui finissait par 12, puisque le cavalier peut sauter de 12 à ces cases 59, 41, 11 et 13, fournira ces transformées:

1.....11.32.....59.12.....31.64.....60,
1.....11.32.....41.12.....31.64.....42,

et celle-là, puisque 60 conduit aux cases 61, 59, 9, 45, 25, 27, 13 et 53, nous mènera à plusieurs nouvelles routes, où les dernières cases seront 10, 46, 26, 28, 14 et 54.

13. Voilà donc une source bien riche d'où l'on peut puiser quantité de nouvelles routes, en ayant une fois trouvé une seule: et le nombre des transformations devient encore plus grand, quand on renverse l'ordre de la première route en sorte

64.........1,

où la dernière case tenant à 52 fournit cette transformée

64.....52.1.....51

et puisque 51 donne un saut à 64, cette route est rentrante en elle-même, mais elle n'est que la renversée de celle de ci-dessus. Or 51 étant lié avec 64, 52, 54, 56, 26 et 50, fournit ces transformées

64.....54.51.....1.52.53,

64.....56.51.....1.52..55,

64.....52.1.....26.51.....27,

et de celles-ci, si l'on veut, on peut encore trouver quantité d'autres, parmi lesquelles on ne manquera pas d'en découvrir qui sont rentrantes en elles-mêmes.

14. Or, en ayant déjà trouvé une, qui est rentrante en elle-même, comme est celle du § 6, il n'est pas difficile d'en trouver plusieurs autres de même nature: on n'a qu'à arranger les cases en sorte, que tant la première que la dernière, se trouve éloignée des bandes, puisqu'alors l'une et l'autre permet huit sauts. Ainsi, si nous rangeons les nombres de la route § 6 en sorte

31.....64.1.....30

la dernière case 30 étant jointe à celles-ci: 45, 59, 23, 29, 31, 13, 43, 41, fournit ces transformées:

I. 31.....45.30.....1.64.....46,

II. 31.....59.30.....1.64.....60,

III. 31.....64.1.....23.30.....24,

IV. 31.....64.1.....13.30.....14,

V. 31.....43.30.....1.64.....44,

VI. 31.....41.30.....1.64.....42,

où la II et la IV sont rentrantes en elles-mêmes, et tant de celles-ci que des autres on pourra trouver, par des transformations ultérieures, plusieurs autres. Ainsi la troisième donne

31........64.1.......13.24.....30.23.....14

31..33.24......30.23......1.64.......34

31........64.1.......15.24.....30.23....16.

15. Mais quand on n'a pas encore une route de la première espèce, voyons comment il faut s'y prendre pour en trouver une, sans se livrer au seul hasard. En commençant par une case quelconque, qu'on continue à volonté les sauts du cavalier aussi loin qu'on pourra, et qu'on mette dans les cases qui sont restées vides, des lettres qui leur servent de signe, comme dans cette figure:

34	21	54	9	32	19	48	7
55	10	33	20	53	8	31	18
22	35	62	*a*	40	49	6	47
11	56	41	50	59	52	17	30
36	23	58	61	42	39	46	5
57	12	25	38	51	60	29	16
24	37	2	43	14	27	4	45
1	*b*	13	26	3	44	15	28

Ici j'ai pu continuer la route jusqu'à la case marquée par 62.

16. Maintenant, ayant 62 cases parcourues par le cavalier, je les représente de cette manière: 1 . . . . 62, et regardant la case 62 comme la dernière, je cherche des transformées, qui finissent par d'autres cases, d'où il y ait un passage sur l'une des cases *a* ou *b*. Or la case 62 communique avec celles-ci 9, 53, 59, 61, 23, 11, 55 et 21, d'où nous tirons ces transformées:

I. 1 . . . . . 9.62 . . . . . 10, d'où l'on passe en *a*

II. 1 . . . . 53.62 . . . . . 54, d'où l'on passe en *a*

III. 1 . . . . 59.62 60

IV. 1 . . . . 23.62 24

V. 1 . . . . 11.62 12

VI. 1 . . . . 55.62 . . . . . 56, d'où l'on passe en *a*

VII. 1 . . . . 21.62 . . . . . 22.

Donc les routes I, II et VI s'étendent déjà jusqu'à la case *a*, et il n'y reste plus vide que la seule case *b*, et pour la lier avec les autres on n'a qu'à transformer une de ces trois routes par la même méthode. On opérerait semblablement s'il était resté plusieurs cases vides.

17. Prenons la première transformée

1 . . . . . 9.62 . . . . . 10.*a*

dont la dernière case *a* conduit à 32, 8, 52, 42, 58, 56, 10 et 54, parmi lesquelles 58 fournit cette transformée

1 . . . . . 9.62 . . . . . 58.*a*.10 57

dont la dernière 57 conduit à la case *b*, de sorte qu'à présent le cavalier aura parcouru toutes les cases, ayant commencé sa course en 1, et fini en *b*.

1 . . . . . 9.62 . . . . . 58.*a*.10 . . . . . 57.*b*.

Mais cette route n'est pas rentrante en elle-même. Pour lui procurer cet avantage, cherchons de nouvelles transformées, la dernière case *b* conduisant à ces cases 57, 25, 43, dont 25 donne cette transformée

1 . . . . . 9.62 . . . . . 58.*a*.10 . . . . . 25.*b*.57 26,

où la dernière conduit à 37, 25, 51 et 27. Or, aucune ne fournit une route de la seconde espèce. Prenons donc 43:

1 . . . . . 9.62 . . . . . 58.*a*.10 . . . . . 43.*b*.57 44

dont la dernière 44 conduit à 43, 51, 29 et 45, dont aucune ne donne immédiatement une route rentrante en elle-même.

18. Il faudra donc passer à de nouvelles transformées, et pour que cela se puisse faire plus aisément, il sera bon de présenter la route trouvée de la première espèce par l'ordre naturel des nombres:

40	27	60	9	38	25	54	7
61	16	39	26	59	8	37	24
28	41	10	15	46	55	6	53
17	62	47	56	13	58	23	36
42	29	14	11	48	45	52	5
63	18	31	44	57	12	35	22
30	43	2	49	20	33	4	51
1	64	19	32	3	50	21	34

où la route étant représentée en sorte

1 64,

et la dernière case 64 conduisant à 63, 31, 49, on aura deux transformées

I. 1 . . . . . 31.64 32

II. 1 . . . . . 49.64 50,

car la case 63 ne change rien dans la proposée.

19. Puisqu'il n'y a que deux cases qui aboutissent à la première 1, renversons ces deux transformées pour avoir

I. 32 . . . . . 64.31 1

II. 50 . . . . . 64.49 1

et maintenant la dernière 1 conduisant à 2 et 18, nous en tirons ces deux nouvelles

A. 32 . . . 64.31 . . . 18.1 . . . 17

B. 50 . . . 64.49 . . . 18.1 . . . 17

où la dernière 17 conduisant à 16, 10, 14 et 18, nous obtiendrons

C. 32 . . . 64.31 . . . 18.1 . . . 10.17 . . . 11

D. 50 . . . 64.49 . . . 18.1 . . . 10.17 . . . 11

E. 32 . . . 64.31 . . . 18.1 . . . 14.17 . . . 15

F. 50 . . . 64.49 . . . 18.1 . . . 14.17 . . . 15

La dernière 11 conduit à 46, 58, 12, 20, 2, 18, 62 et 10, et donne

G. 32 . . . 46.11 . . . 17.10 . . . 1.18 . . . 31.64 . . . 47

H. 50 . . . 64.49 . . . 46.11 . . 17.10 . . . . 1.18 . . . 45

J. 32 . . . 58.11 . . . 17.10 . . . 1.18 . . . 31.64 . . . 59

K. 50 . . . 58.11 . . . 17.10 . . . 1.18 . . . 49.64 . . . 59

L. 32 . . . 64.31 . . . 20.11 . . 17.10 . . . 1.18.19

M. 50 . . . 64.49 . . . 20.11 . . 17.10 . . . 1.18.19

N. 32 . . . 64.31 . . . 18.1.2.11 . . . 17.10 . . . 3

O. 50 . . . 64.49 . . . 18.1.2.11 . . . 17.10 . . . 3

P. 32 . . . 62.11 . . . 17.10 . . . 1.18 . . 31.64.63

Q. 50 . . . 62.11 . . . 17.10 . . . 1.18 . . . 49.64.63.

20. Or E et F, dont la dernière case 15 conduit à 33, 8, 58, 48, 14, 62, 16 et 60, donneront ces transformées:

g. 32 ... 38.15 ... 17.14 ... 1.18 ... 31.64 ... 39
h. 50 ... 64.49 ... 38.15 .. 17.14 .... 1.18 ... 37
i. 32 ... 64.31 ... 18.1 .... 8.15 ... 17.14 9
k. 50 ... 64.49 ... 18.1 .... 8.15 ... 17.14 9
l. 32 ... 58.15 ... 17.14 ... 1.18 ... 31.64 ... 59
m. 50 ... 58.15 ... 17.14 ... 1.18 ... 49.64 ... 59
n. 32 ... 48.15 ... 17.14 ... 1.18 ... 31.64 ... 49
o. 50 ... 64.49.48 15 ... 17.14 ... 1.18 ... 47
p. 32 ... 62.15 ... 17.14 ... 1.18 ... 31.64.63
q. 50 ... 62.15 ... 17.14 ... 1.18 ... 49.64.63
r. 32 ... 60.15 ... 17.14 ... 1.18 ... 31.64 ... 61
s. 50 ... 60.15 ... 17.14 ... 1.18 ... 49.64 ... 61.

Mais parmi toutes ces transformées il ne s'en trouve pas encore une qui soit rentrante en elle-même, mais leurs transformées ultérieures en fourniront assez.

21. Prenons la route indiquée par la lettre G, où la dernière case 47 communiquant avec celles-ci: 26, 46, 48, 44, 18, 42, 28 et 16, les dernières cases qu'on aura par ces transformations seront: 27, 11, 47, 45, 19, 43, 29 et 17, dont 43 communique avec la première 32, et donne, par conséquent, cette route rentrante:

32 ... 42.47 ... 64.31 ... 18.1 ... 10.17 ... 11.46 ... 43

laquelle pourra donc être représentée en sorte

1 ... 10.17 ... 11.46 ... 43.32 ... 42.47 ... 64.31 ... 18,

et marquant les cases par l'ordre naturel des nombres, on aura cette route rentrante:

30	55	46	9	28	57	40	7
47	12	29	56	45	8	27	58
54	31	10	13	18	41	6	39
11	48	33	42	15	44	59	26
32	53	14	17	34	19	38	5
49	64	51	20	43	16	25	60
52	21	2	35	62	23	4	37
1	50	63	22	3	36	61	24

22. La route indiquée par la lettre H ayant 45 pour sa dernière case, les cases communiquantes sont: 6, 36, 22, 4, 20, 44, 56, 46
et les dernières seront: 5, 37, 23, 3, 21, 45, 57, 11

où 57 communique avec la première 50, d'où résulte cette route rentrante:

50 ... 56.45 ... 18.1 ... 10.17 ... 11.46 ... 49.64 ... 57

qui pourra aussi être représentée en sorte

1 ... 10.17 ... 11.46 ... 49.64 ... 57.50 ... 56.45 ... 18.

42	55	26	9	44	57	34	7
25	12	43	56	27	8	45	58
54	41	10	13	18	35	6	33
11	24	19	36	15	28	59	46
40	53	14	17	20	37	32	5
23	64	51	38	29	16	47	60
52	39	2	21	62	49	4	31
1	22	63	50	3	30	61	48

qui ne diffère pas beaucoup de la précédente.

23. Les routes indiquées par J et K ayant la dernière case 59, on aura

les cases communiquantes: 54, 6 58, 56, 10, 60

les dernières pour J seront: 55, 5, 11, 57, 9, 59

Or les dernières pour K: 55, 5, 11, 57, 9, 59

d'où nous tirons encore deux rentrantes, puisque 57 communique tant avec 32 qu'avec 50, savoir

32 ... 56.59 ... 64.31 ... 18.1 ... 10.17 ... 11.58.57

50 ... 56.59 ... 64.49 ... 18.1 ... 10.17 ... 11.58.57

qui pourront être représentées en sorte

1 ... 10.17 ... 11.58.57.32 ... 56.59 ... 64.31 ... 18

1 ... 10.17 ... 11.58.57.50 ... 56.59 ... 64.49 ... 18.

De même, les routes L et M finissant par 19, on aura

les cases communiquantes avec 19 „ „ 30, 18, 44, 20

de là les dernières pour L „ „ „ „ 29, 19, 45, 11

pour M „ „ „ „ 29, 19, 43, 11

où il n'y a aucune rentrante. Les routes N et O finissant par 3, on aura par rapport à cette dernière:

les cases communiquantes „ „ „ „ 2, 44, 12, 4

alors la dernière devient pour N „ „ 11, 45, 13, 3

pour O „ „ 11, 43, 13, 3

où il n'y en a point non plus.

24. S'il valait la peine, on pourrait, en poursuivant ces transformations, trouver plusieurs autres routes rentrantes en elles-mêmes, et on ne manquerait pas de découvrir des moyens pour abréger les opérations, en achevant deux ou plusieurs à la fois, afin qu'on arrive plus tôt au but

proposé. Aussi n'est ce pas mon dessein d'assigner toutes les routes possibles qui soient rentrantes en elles-mêmes, ce qui serait un ouvrage aussi pénible qu'inutile; je me contente d'avoir donné une méthode sûre pour trouver autant de routes qu'on voudra, méthode dont l'application n'est pas difficile en chaque cas. Mais on peut ajouter à la question principale encore des conditions qui la rendent plus curieuse: comme, si l'on exigeait que les nombres, qui se trouvent dans des cases opposées, aient entr'eux la même différence qui doit être 32, comme étant la moitié du nombre de toutes les cases. Or, chaque case en a une qui lui est opposée, de sorte que la ligne droite tirée par les centres de ces deux cases divise le quarré en deux parties égales. On demande donc que les nombres 33, 34, 35, 36 .... 64 se trouvent à l'opposite des nombres 1, 2, 3, 4 ... 32.

25. Pour trouver de telles routes diagonales, on n'a qu'à commencer par écrire les nombres 1, 2, 3, 4 etc. conformément à la marche du cavalier, et à mesure qu'on écrit ces nombres, mettre les nombres 33, 34, 35, 36 etc. dans les cases opposées, et poursuivre cet arrangement tant qu'on pourra: comme on peut le voir par la figure ci-jointe

10	29	48	35	8	31	46	33
49	36	9	30	47	34	7	58•
28	11	*A*	*C*	*f*	45	32	19•
37	50	*B*	*D*	*e*	6	59	44
12	27	38	*E*	*d*	*b*	18	5
51•	64	13	*F*	*c*	*a*	43	60
26•	39	2	15	62	41	4	17
1	14	63	40	3	16	61	42

Ici j'ai pu continuer la suite des nombres 1, 2, 3, jusqu'à 19, et celle des nombres 33, 34, 35, jusqu'à 51. Mais en rétrogradant je suis passé de 1 par 64, 63 jusqu'à 58, et de 33 j'ai pu reculer jusqu'à 26. Douze cases sont restées vides; je les remplies des lettres *A*, *a*, *B*, *b*, *C*, *c*, *D*, *d*, *E*, *e*, *F*, *f*, disposées par des cases opposées.

26. Nous avons donc deux séries séparées de cases qui se suivent selon la marche du cavalier:

58 ..... 64.1 19

26 .... 51.

La case 19 aboutissant à 6, nous aurons ces transformées qui pourront être continuées plus loin:

58 ..... 64.1 ..... 6.19 ..... 7.*f*.*B*.*d*.*C*,

26 ..... 38.51 ...... 39.*F*.*b*.*D*.*c*.

Maintenant, la case *C* communiquant aux cases de la première suite 8, 6, *d*, ne fournit pas de nouvelles transformations. Mais retranchons les deux dernières, et puisqu'il suffit de transformer une seule suite, parce que l'autre en est déterminée, prenons la première

58 .... 64.1 ..... 6 19 ..... 7.*f*.*B*

où *B* aboutissant à 12 donne cette transformée à continuer

58 . . . 64.1 . . . 6.19 . . . 12.*B*.*f*.7 . . . 11.*D*.*c*.

Or *c* étant communicable à 16, on aura

58 . . . 64.1 . . . 6.19 . . . 16.*c*.*D*.11 . . . 7.*f*.*B*.12 . . . 15.*a*.*E*;

et l'autre suite sera

26 . . . . . 38.51 . . . . . 48.*C*.*d*.43 . . . . . 39.*F*.*b*.44 . . . 47.*A*.*e*,

où toutes les cases sont comprises.

27 Maintenant il faut lier ces deux suites ensemble, en sorte que la fin de l'une aboutisse au commencement de l'autre. Pour cet effet, transformons la première dont la fin *E* communique avec la case 62, et la fin devenant alors 63, sera cohérente avec le commencement de l'autre 26. Cette transformation donne donc:

58 . . . 62.*E*.*a*.15 . . . 12.*B*.*f*.7 . . . 11.*D*.*c*.16 . . . 19.6 . . . 1.64.63

26 . . . 30.*e*.*A*.47 . . . 44.*b*.*F*.39 . . 43.*d*.*C*.48 . . . 51.38 31

et on a en même temps une route rentrante en elle-même et douée de la condition préscrite:

14	59	42	35	16	31	54	33
41	36	15	58	55	34	17	30
60	13	56	43	18	53	32	7
37	40	19	12	57	6	29	52
20	61	38	25	44	51	8	5
39	64	21	50	11	24	45	28
62	49	2	23	26	47	4	9
1	22	63	48	3	10	27	46

28. Ayant trouvé une seule route de cette nature, il est aisé de la transformer en plusieurs manières différentes en lui conservant la même propriété. Car, de quelque manière qu'on partage la suite rentrante des nombres 1 . . . . . 64 en deux moitiés, l'une contient toujours les cases opposites de l'autre, comme on peut le voir par ces bissections:

1 32	2 33	3 34	4 35
33 64	34 . . . 64.1	35 . . . 64.1.2	36 . . . 64.1 . . 3

où les deux moitiés sont toujours cohérentes. Maintenant, on n'a qu'à prendre une telle bissection à volonté, et transformer les deux moitiés semblablement, jusqu'à ce qu'elles redeviennent cohérentes. Ainsi, prenons la moitié 3 . . . . 34 dont le bout 34 communiquant à 7 donne la transformée 3 . . . 7.34 . . . 8, et par renversement 8 . . . 34.7 . . . 3 dont le bout 3 communiquant à 24 donne 8 . . . . 24.3 . . . 7.34 . . . . 25, et l'autre moitié sera

40 . . . . 56.35 . . . 39.2.1.64 57

qui sont coherentes pas leurs bouts 25, 40 et 8, 57. Nous pourrons donc représenter en sorte cette nouvelle route

1.2.39 . . . 35.56 . . . . 40.25 32

33.34.7 . . . . 3.24 . . . . . 8.57 . . . . 64.

29. La même moitié 3 . . . . . 34, puisque le premier bout 3 communique à 24, donne par la transformation:

23 . . . . . 3.24 34,

et 34 communiquant à 7 donne

23 . . . . . 7.34 . . . . . 24.3 . . . 6

et l'autre moitié sera

55 . . . . . 39.2.1.64 . . . 56.35 . . . 38

qui est cohérente. Par conséquent, nous aurons une route représentée par ces deux moitiés:

1.2.39 . . . . . 55.6 . . . 3.24 32

33.34.7 . . . . . 23.38 . . 35.56 . . . . 64.

La moitié 4 . . . . . 35, à cause de la communication du bout 35 avec 18, donne

4 . . . . . 18 35 19

qui est déjà cohérente avec

36 . . . . . 50.3 . . 1.64 51

d'où nous tirons cette route

1 . . . 3.50 . . . . . 36.19 32

33 . . 35.18 . . . . . . 4.51 64

et d'autres transformations de la même moitié donnent

1 . . . 3.50 . . . 43.36.19 . . . 23.10 . . . 5.24 . . . 32

33 . . 35.18 . . . 11.4.51 . . . 55.42 . . 37.56 . . . 64.

30. Voilà donc quatre autres routes qui ont la même propriété que celle du § 27:

50	59	22	7	48	31	10	33
23	6	49	58	9	34	47	30
60	51	8	21	46	11	32	35
5	24	45	52	57	36	29	12
44	61	4	25	20	13	56	37
3	64	43	14	53	40	19	28
62	15	2	41	26	17	38	55
1	42	63	16	39	54	27	18

42	59	6	55	44	31	18	33
5	54	43	58	19	34	45	30
60	41	56	7	46	17	32	35
53	4	47	40	57	20	29	16
48	61	52	25	8	15	36	21
3	64	49	14	39	24	9	28
62	13	2	51	26	11	22	37
1	50	63	12	23	38	27	10

40	59	12	35	38	31	54	33
13	18	39	58	55	34	37	30
60	41	56	11	36	53	32	47
17	14	19	42	57	48	29	52
20	61	16	25	10	51	46	49
15	64	21	4	43	24	9	28
62	5	2	23	26	7	50	45
1	22	63	6	3	44	27	8

40	59	50	35	38	31	48	33
51	12	39	58	49	34	37	30
60	41	56	11	36	47	32	21
55	52	13	42	57	22	29	46
14	61	54	25	10	45	20	23
53	64	15	4	43	24	9	28
62	5	2	17	26	7	44	19
1	16	63	6	3	18	27	8

31. A cette condition des cases opposées on peut encore ajouter celle-ci, que la première moitié des nombres 1 ..... 32 remplisse seule la moitié du quarré, en partageant le quarré par une ligne parallèle à un côté

							33

α ———————————————— β

1	*a*	*b*	28	7	14	19	16
24	27	8	*c*	20	17	6	13
9	2	25	22	11	4	15	18
26	23	10	3	*d*	21	12	5

en sorte que les nombres 1 ..... 32 se trouvent tous au-dessous de la ligne $\alpha\beta$, et les autres 33 ..... 64 au-dessus. Il faut donc que l'unité se trouve près de la ligne $\alpha\beta$, afin qu'elle puisse communiquer avec le nombre 64 qui se trouvera au-dessus.

32. Commençons donc par mettre l'unité à une telle case quelconque, et en vertu de l'opposition, la case du nombre 33 sera aussi déterminée, et il faudra faire en sorte quelle communique avec celle qui contiendra le nombre 32 au dessous de la ligne $\alpha\beta$. En essayant une telle disposition, je suis parvenu jusqu'au nombre 28, et j'ai écrit dans les cases vides les lettres *a*, *b*, *c*, *d*, pour l'arrangement desquelles je fais les transformations suivantes. La suite 1 ..... 28, puisque 28 aboutit à 27, 25, 11, 17, donne ces transformées:

I. 1 ..... 25.28 ... 26

II. 1 ..... 11.28 12

III. 1 ..... 17.28 18

dont aucune ne s'étend à une des cases vides. Mais après plusieurs transformations on parvient à celle-ci qui comprend toutes les cases:

1 .... 8.23 . . 21.18 . . 20.*b*.24 ... 28.17 .... 9.*a*.*c*.*d*.

qui se transforme enfin en celle-ci

1 .... 8.23 . . 21.18 . . 20 *b*.24 ... 28.17 . . 15.*d*.*c*.*a*.9 14

dont la fin 14 communique avec le commencement 33 de l'autre moitié au-dessus de la ligne $\alpha\beta$: et la fin de celle-ci 64 communiquera d'elle même avec la case 1.

33. Voici donc cette route représentée en son entier:

37	62	43	56	35	60	41	50
44	55	36	61	42	49	34	59
63	38	53	46	57	40	51	48
54	45	64	39	52	47	58	33

α ——— β

1	26	15	20	7	32	13	22
16	19	8	25	14	21	6	31
27	2	17	10	29	4	23	12
18	9	28	3	24	11	30	5

et il est non seulement aisé d'en trouver, par la même méthode, plusieurs autres, mais on peut aussi transformer celle-ci en plusieurs manières, dont voici quelques unes:

7 . . . . . 1 . 8 32

7 . . . . . 1 . 8 . . . . . 25 . 32 26

15 . . . . 10 . 7 . . . . 1 . 8 . 9 . 16 . . . 21 . 24 . . . . 32 . 23 . 22

qu'on peut encore renverser, de même que la primitive, en la représentant en sorte 32 . . . . . 1.

34. Voilà donc encore quelques routes de cette espèce:

35	62	43	56	37	60	41	50
44	55	36	61	42	49	38	59
63	34	53	46	57	40	51	48
54	45	64	33	52	47	58	39

α ——— β

7	26	15	20	1	32	13	22
16	19	8	25	14	21	2	31
27	6	17	10	29	4	23	12
18	9	28	5	24	11	30	3

35	60	43	56	37	62	41	50
44	55	36	61	42	49	38	63
59	34	53	46	57	40	51	48
54	45	58	33	52	47	64	39

α ——— β

7	32	15	20	1	26	13	22
16	19	8	25	14	21	2	27
31	6	17	10	29	4	23	12
18	9	30	5	24	11	28	3

41	60	37	54	43	58	47	50
36	63	42	59	38	49	44	57
61	40	53	34	55	46	51	48
64	35	62	39	52	33	56	45

α ——— β

13	24	1	20	7	30	3	32
16	19	14	23	2	21	8	29
25	12	17	6	27	10	31	4
18	15	26	11	22	5	28	9

62	37	56	41	60	35	54	47
57	42	61	36	55	48	51	34
38	63	44	59	40	53	46	49
43	58	39	64	45	50	33	52

α ——— β

20	1	18	13	32	7	26	11
17	14	21	8	27	12	31	6
2	19	16	23	4	29	10	25
15	22	3	28	9	24	5	30

35. Jusqu'ici j'ai considéré la question telle qu'elle avait été proposée pour l'échiquier ordinaire divisé en 64 cases. Or comme ce nombre est trop grand, pour qu'on puisse concevoir toutes les variétés qui y peuvent avoir lieu, il sera bon de considérer aussi quelques figures plus simples, qui contiennent un moindre nombre de cases que le cavalier d'échecs doive parcourir. Or, d'abord il est évident, que ni un quarré de 4, ni un de 9 cases n'y est propre: mais on verra qu'on ne saurait réussir non plus dans un quarré de 16 cases.

1	8	13	10
14	11	4	7
5	2	9	12
	15	6	3

Car, de quelque manière qu'on s'y prenne, il restera toujours une case angulaire vide, et on s'apercevra bientôt, que toutes les transformations qu'on puisse faire ne sont pas capables de la remplir. Il est clair qu'on devrait commencer et finir par un coin: et partant deux des quatre cases du milieu seront d'abord remplies, et les deux autres devraient être gardées jusqu'à la fin, ce qui ne se peut pas.

36. Le premier quarré donc que le cavalier puisse parcourir, est celui de 25 cases, qu'on pourra remplir moyennant les mêmes règles, en cas qu'on ne réussisse point au premier essai.

7	12	17	22	5
18	23	6	11	16
13	8	25	4	21
24	19	2	15	10
1	14	9	20	3

Or, la marche du cavalier produit toujours cette propriété que les nombres pairs et impairs se suivent alternativement, comme on peut le voir par toutes les figures rapportées jusqu'ici. D'où il est évident que la dernière case contenant 25 ne saurait jamais communiquer avec la première 1: et partant, il est impossible de trouver une route rentrante en elle-même dans le quarré de 25, ni dans aucune autre figure qui contient un nombre impair de cases. On comprend de là aussi, qu'on ne saurait jamais commencer par une case qui contient un nombre pair; car de quelque manière qu'on transforme cette route, les nombres pairs tomberont toujours dans les mêmes cases, et les cases angulaires contiendront des nombres impairs. Dans ce quarré de 25 il est aussi clair, qu'il faut absolument ou commencer ou finir par une case angulaire.

37. Mais voyons aussi les transformations qu'on peut tirer de cette route 1 . . . . . 25 trouvée du quarré de 25 cases. Or, la dernière communiquant aux cases 20, 10, 16, 22, 12, 18, 24 et 14, fournit ces transformées:

I. 1....20.25....21, II. 1....10.25....11,
III. 1....16.25....17, IV. 1....22.25....23,
V. 1....12.25....13, VI. 1....18.25....19,
VII. 1.......25, VIII. 1....14.25....15.

Donc, commençant par la case angulaire, on peut finir par l'une quelconque de ces cases 21, 11, 17, 23, 13, 19, 25, 15. Mais la première donne encore ces transformées:

a. 1....6.21...25.20....7, *b.* 1.2.21....25.20....3,

et les autres celles-ci

c. 1.2.11...25.10...3, *d.* 1...8.11...25.10.9,
e. 1...4.17...25.16...5, *f.* 1...8.17...25.16...9,
g. 1...4.23...25.22...5, *h.* 1.2.23...25.22....3,
i. 1...6.13...25.12...7, *k.* 1.2.13...25.12...3,
l. 1...6.19...25.18...7, *m.* 1...4.19...25.18...5,
n. 1...6.15...25.14...7, *o.* 1...8.15...25.14...9,

où les dernières cases sont 3, 5, 7, 9.

38. Puisque les cases angulaires 3, 5, 7 ne communiquent qu'à deux autres, elles ne fournissent point, par notre méthode, de nouvelles transformées. Considérons donc celles qui finissent par 9, et nous tirerons ces transformées:

p. 1...4.9.10.25...11.8...5, *q.* 1...8.11...24.9.10.25,
r. 1...4.9...16.25...17.8..5, *s.* 1...8.17...24.9...16.25,
t. 1...4.9...14.25...15.8..5, *u.* 1...8.15...24.9...14.25.

Maintenant ces nouvelles routes, qui finissent par 25, nous conduisent à d'autres transformées, et nous parviendrons à plusieurs autres routes qui finissent par une quelconque des cases qui sont marquées des nombres impairs: d'où l'on voit qu'en commençant par la case angulaire 1, on peut finir par quelque case marquée d'un nombre impair qu'on voudra, et cela en plusieurs manières différentes. Ensuite, chaque route pouvant être renversée, le nombre de toutes les routes possibles deviendra extrêmement grand.

39. Ici on peut encore ajouter cette condition: que les nombres qui se trouvent en deux cases opposées, fassent partout la même somme, savoir 26. Il faut donc que la première et dernière cases se trouvent en des angles opposés; et pour trouver une telle route, on n'a qu'à commencer à remplir le quarré, et mettre à l'opposite de chaque nombre son complément à 26, et continuer aussi loin qu'on pourra.

23	18	5	10	25
6	11	24	19	14
17	22	13	4	9
12	7	2	15	20
1	16	21	8	3

Mais puisqu'on sait que la case du milieu doit contenir 13, on ne saurait presque manquer; et alors, en conservant la même propriété, on en peut tirer plusieurs formes différentes dont voici quelques unes:

I. 1 . . . 4 . 11 . . . 5 . 14 . **13** . 12 . 21 . . . 15 . 22 . . . 25,

II. 1 . . . 4 . 7 . . 5 . 14 . . 18 . **13** . 8 . . . 12 . 21 . . 19 . 22 . . 25,

III. 1 . . . 4 . 21 . . . . 14 . **13** . 12 . . . 5 . 22 . . . 25,

IV. 1 . . . 5 . 14 . . . . 20 . **13** . 6 . . . 12 . 21 . . . 25,

V. 1 . . 4 . 11 . 12 . 21 . . . 16 . **13** . 10 . . . 5 . 14 . 15 . 22 . . . 25,

VI. 1 . . 4 . 7 . . . 12 . 21 . 20 . **13** . 6 . 5 . 14 . . . 19 . 22 . . . 25,

VII. 1 . . 4 . 21 . 12 . . . . 6 . **13** . 20 . . . 14 . 5 . 22 . . . 25.

40. Dans toutes ces variations, tant les quatre premiers nombres 1 . . . 4 que les quatre derniers 22 . . . 25, avec celui du milieu 13, demeurent invariables, de sorte que les variations ne s'étendent que sur les autres. D'où il semble aussi que la route trouvée avec les sept variations épuisent entièrement cette espèce: voici donc toutes ces huit routes représentées à la fois:

23	18	5	10	25
6	11	24	19	14
17	22	13	4	9
12	7	2	15	20
1	16	21	8	3

23	18	11	6	25
10	5	24	17	12
19	22	13	4	7
14	9	2	21	16
1	20	15	8	3

23	12	7	16	25
6	17	24	21	8
11	22	13	4	15
18	5	2	9	20
1	10	19	14	3

23	8	21	16	25
20	15	24	7	12
9	22	13	4	17
14	19	2	11	6
1	10	5	18	3

23	10	19	14	25
18	5	24	9	20
11	22	13	4	15
6	17	2	21	8
1	12	7	16	3

23	20	15	8	25
14	9	24	21	16
19	22	13	4	7
10	5	2	17	12
1	18	11	6	3

23	16	21	8	25
12	7	24	15	20
17	22	13	4	9
6	11	2	19	14
1	18	5	10	3

23	10	5	18	25
14	19	24	11	6
9	22	13	4	17
20	15	2	7	12
1	8	21	16	3

41. Les routes trouvées ci-dessus pour un quarré de 25 cases se peuvent ainsi disposer qu'elles remplissent un quarré de 100 cases, en sorte que la route devienne rentrante en elle-même. Voici un tel quarré de 100 cases:

30	41	46	37	32	53	60	67	72	55
47	36	31	40	45	68	73	54	61	66
42	29	38	33	50	59	52	63	56	71
35	48	27	44	39	74	69	58	65	62
28	43	34	49	26	51	64	75	70	57
7	20	25	14	1	76	99	84	93	78
12	15	8	19	24	89	94	77	98	85
21	6	13	2	9	100	83	88	79	92
16	11	4	23	18	95	90	81	86	97
5	22	17	10	3	82	87	96	91	80

où les nombres sont disposés en quatre quartiers dont chacun contient la même route.

42. Avant que de finir, j'ajouterai encore quelques autres figures, et parmi les rectangulaires, la plus simple que le cavalier puisse parcourir est de 12 cases, la largeur contenant 3, et la longueur 4, dont voici quelques routes:

10	7	2	5
1	4	9	12
8	11	6	3

3	6	11	8
12	9	2	5
1	4	7	10

3	6	9	12
8	11	2	5
1	4	7	10

12	9	6	3
1	4	11	8
10	7	2	5

Mais on voit aisément que des routes rentrantes ne sauraient ici avoir lieu. Si la largeur contient trois cases, et la longueur 5 ou 6, il est impossible de les parcourir: mais donnant à la longueur 7 ou plusieurs cases, on pourra réussir, pourtant sans rentrer:

3	8	5	18	15	10	13
6	19	2	9	12	21	16
1	4	7	20	17	14	11

15	18	21	2	5	8	11
20	1	16	13	10	3	6
17	14	19	4	7	12	9

Or, si nous donnons 4 cases à la largeur, et 5 ou plusieurs à la longueur, on aura ces routes:

14	7	20	3	16
19	2	15	8	11
6	13	10	17	4
1	18	5	12	9

16	7	22	3	18	11
23	2	17	12	21	4
8	15	6	19	10	13
1	24	9	14	5	20

20	7	26	13	18	5	24
27	14	19	6	25	12	17
8	21	2	15	10	23	4
1	28	9	22	3	16	11

43. Jusqu'ici les routes rentrantes en elles-mêmes ne peuvent pas avoir lieu; mais, donnant 5 cases à la largeur, et 6 à la longueur, on pourra aussi remplir cette condition, de même que

dans tous les autre rectangles, dont le nombre des cases est pair, pourvu qu'il n'y ait pas moins de 5 cases dans un côté. En voici des exemples:

3	20	13	24	5	18
12	29	4	19	14	25
21	2	23	8	17	6
28	11	30	15	26	9
1	22	27	10	7	16

30	21	6	15	28	19
7	16	29	20	5	14
22	31	8	35	18	27
9	36	17	26	13	4
32	23	2	11	34	25
1	10	33	24	3	12

où cette autre figure est un carré de 36 cases, et la route est non seulement rentrante en elle-même, mais les nombres dans les cases opposées ont partout la même différence de 18.

44. Mais, sans se borner aux figures rectangulaires, on peut former à volonté quantité d'autres figures, où le cavalier peut passer par toutes les cases: j'en ajouterai quelques unes, qui sont plus simples, et qui admettent même des routes rentrantes en elle-mêmes:

	10	7	
12	5	2	9
3	8	11	6
	1	4	

		14	19		
		7	12		
6	13	20	15	18	11
1	8	5	10	3	16
		2	17		
		9	4		

	1	14	7	22	
15	8	21	32	13	24
2	31	26	23	6	19
9	16	29	20	25	12
30	3	10	27	18	5
	28	17	4	11	

	1	20	7	26	
21	8	27	32	19	14
2	29	12	15	6	25
9	22	31	28	13	18
30	3	16	11	24	5
	10	23	4	17	

XXV.

De numeris primis valde magnis.

(N. Comment. IX. 1762 — 63 p. 99. Exhib. 1760. Dec. 1.)

Vix ullus reperietur geometra, qui non, ordinem numerorum primorum investigando, haud parum temporis inutiliter consumserit: videtur enim lex, qua numeri primi progrediuntur, in arithmetica aeque abstrusae esse indaginis, atque in geometria circuli quadratura: ac si hujus indagatio pro desperata est habenda, non leviores adsunt rationes, quae et ordinis, quo numeri primi se invicem sequuntur, cognitionem nos in perpetuum fugere persuadent. Cum deinde etiam circuli quadratura, quamvis innotesceret, vix quicquam utilitatis allatura perhibeatur, eodem jure negare licebit, ex ordine numerorum primorum perspecto ullum usum esse redundaturum. Verum tamen nemo facile dubitabit, quin methodus ipsa, quae nos vel ad circuli quadraturam, vel ad legem progressionis numerorum primorum manuduceret, quoniam hae res tam diu frustra sunt anquisitae, eximium usum sit praestatura, propterea quod maxima impedimenta quibus hae investigationes adhuc fuerunt implicatae, feliciter superaverit; ita ut inde omni jure summa subsidia per totam mathesin nobis polliceri possemus. Haec ideo monenda duxi, ne quis eos, qui forte in hoc studio desudaverint, reprehendendos censeat. Ac profecto natura numerorum primorum, cum ex iis modo tam admirabili omnes numeri componantur, per se praeclarissima videtur, et quo magis adhuc in proprietates, quibus sunt praeditae, penetrare licuit, eo magis haec doctrina digna censeri debet, cui excolendae plus operae tribuatur, quam nunc quidem plerumque fieri solet. In hoc autem studii genere inprimis excelluit acutissimus quondam Fermatius, cui plurimae insignes numerorum proprietates acceptae sunt referendae; neque parum est dolendum, quod ejus scripta post mortem ita interciderint, ut plurimorum theorematum demonstrationes, quas se adinvenisse asseveraverat, adhuc nobis sint ignotae. Hic perspicacissimus vir in doctrina numerorum primorum etiam non mediocriter laboravit, atque problema se dignissimum olim Wallisio proposuerat, quo modum requirebat, numerum primum dato quovis numero majorem assignandi. Credebat quidem Fermatius, se hujus problematis solutionem in potestate habere, dum affirmaverat, omnes numeros in hac forma 2^n+1 contentos, si quidem exponens n ipse fuerit potestas binarii, esse numeros primos. Verum tamen eo erat candore, ut negaret, se hujus asserti demonstrationem habere, etiamsi de ejus veritate minime dubitaret. Perspicuum autem est, si haec forma 2^n+1, sumendo pro n quasvis binarii potestates, semper numeros primos exhiberet, problema propositum perfecte fore solutum. Quocunque enim numero proposito, non solum una, sed innumerabiles potestates binarii assignari poterunt quae loco exponentis n positae praebiturae sint potestates 2^n dato illo numero majores, ad quas si unitas adjiceretur, haberentur utique totidem numeri primi dato illo numero majores. Hanc autem

regulam a **Fermatio** prolatam veritati non esse consentaneam, jam ante plures annos animadverti. Cum enim pro omnibus casibus inter centena millia subsistentibus satisfaceret, qui sunt:

$$2^1+1=3;\ 2^2+1=5;\ 2^4+1=17;\ 2^8+1=257;\ 2^{16}+1=65537$$

statim sequentem casum $2^{32}+1=4294967297$ non esse primum inveni, sed divisibilem per numerum 641. Quare cum etiam de sequentibus majoribus numeris, ex hac formula natis, incerti simus, utrum sint primi, nec ne? hinc nihil plane adjumenti consequimur ad problema memoratum solvendum. Ac primo quidem nullum est dubium, quin proposito numero quantumvis magno, infiniti adeo existant numeri primi illo majores; postquam jam ab Euclide est demonstratum omnium numerorum primorum multitudinem esse infinitam, etiamsi, ut ego ostendi, haec numerorum primorum multitudo se habeat ad multitudinem omnium prorsus numerorum, ut unitas ad infinitum, seu potius, ut logarithmus numeri infiniti ad ipsum hunc numerum infinitum, quod posterius infinitum majus est, quam postestas quantumvis magna illius infiniti. Solutionis quidem hujus problematis compotes fieremus, si loco formulae 2^n+1 aliam formulam indefinitam detegere liceret, quae nonnisi numeros primos complecteretur; sed etiamsi fortasse talis reperiatur, quae vel centum numeros primos suppeditaret, tamen ei aeque parum confidere possemus pro sequentibus, nisi forte, quod autem vix est expectandum, firma demonstratio exhiberi queat. Nulla certe progressio algebraica datur, cujus omnes plane termini in infinitum crescentes futuri sint numeri primi. Sumto enim termino quocunque, inter sequentes semper infiniti termini ejusdem seriei assignari poterunt, quae omnes per illum dividi queant, quod theorema ita demonstro:

Theorema. Nulla datur progressio algebraica, cujus omnes termini sint numeri primi.

Demonstratio. Cum progressio sit algebraica, posito ejus termino indici x respondente $=X$, erit:

$$X=\alpha+\beta x+\gamma x^2+\delta x^3+\varepsilon x^4+\zeta x^5+\eta x^6+\text{etc.}$$

Posito ergo termino indici a respondente $=A$, ut sit

$$A=\alpha+\beta a+\gamma a^2+\delta a^3+\varepsilon a^4+\zeta a^5+\eta a^6+\text{etc.}$$

si capiatur $x=nA+a$, fiet terminus isti indici respondens X utique per A divisibilis. Omnes ergo progressionis propositae termini, qui indicibus in hac forma $nA+a$ contentis respondent, non erunt numeri primi, neque ergo ulla hujusmodi progressio meros numeros primos complectetur. Q. E. D.

Verum etiamsi non omnes termini hujusmodi progressionis sint numeri primi, problemati tamen satisfieri possit, si modo inter eos infiniti dentur numeri primi, quorum indices certo quodam modo dignoscere liceret; veluti si ejusmodi daretur progressio, cujus omnes termini, quorum indices sunt numeri primi, ipsi essent numeri primi. Sed hoc modo quaerenda esset ejusmodi functio ipsius x, quae, quoties x fuerit numerus primus, ipsa quoque foret numerus primus, vel, quod eodem redit, regula desideraretur, cujus ope ex quovis numero primo proposito inveniri posset novus numerus primus. At hujusmodi regulam profundissimae esse indaginis, quilibet in hujusmodi investigationibus vel leviter versatus facile agnoscet, ita ut hinc nulla plane spes affulgeat, unquam ad solutionem allati problematis Fermatiani perveniendi.

Certum igitur est, in hoc problemate nihil adhuc esse praestitum, postquam ipsius Fermatii conatus successu sint destituti. Atque adeo, cum tabula numerorum primorum nondum ultra centena millia habeatur extensa, problema sane jam non parum foret difficile, si modo numeri primi quaerantur, qui sint centenis millibus majores, vel cum nuper prodierit tabula numerorum primorum usque ad 101000 excurrens, si numeri primi quaerantur hunc terminum superantes. Neque enim ad hoc saltem problema solvendum alia via patere videtur, nisi ut more solito ex numeris ultra 101000 notatis omnes compositi expungantur, hoc est: omnes, qui per ullum numerum primum, radice quadrata minorem, divisibiles deprehendentur; qui numeri enim his expunctis relinquentur, erunt numeri primi. Haec autem operatio instituenda plane foret eadem ratione, ac si ipsam tabulam numerorum primorum ad ulteriores limites continuare vellemus; quod opus propterea esset immensi laboris. Quodsi autem quis forte hunc laborem susciperet, certe non esset expectandum, ut ultra millionem a quoquam produceretur, eoque exantlato omnino impossibile videretur, ullum numerum primum exhibere, qui esset millione major.

Occurrit autem mihi methodus peculiaris, ex qua per calculum non admodum taediosum plures sum adeptus numeros, non solum centies millibus, sed etiam millione majores, quos esse primos certo asseverare possum. Quoniam igitur in tam ardua investigatione leviores successus non sunt contemnendi, haud inutile fore spero, si isthanc methodum meam exposuero, praesertim cum ipsa ex proprietatibus numerorum non spernendis sit derivata, quae etiam in aliis investigationibus usum insignem habere posse videntur.

Deductus autem sum ad hanc methodum per considerationem numerorum quadratorum unitate auctorum, seu in hac formula $aa+1$ contentorum, in quibus, siquidem a sit numerus par, plures numeros primos occurrere manifestum est, sin autem a sit numerus impar, semissis illius formulae $\frac{1}{2}(aa+1)$ plurimos quoque suppeditat numeros primos. Quaesivi ergo omnes divisores numerorum in hac forma $aa+1$ contentorum, qui labor non adeo erat taediosus, cum non opus esset divisionem per omnes numeros primos radice a minores tentare, propterea quod demonstravi, atque id quidem post Fermatium, cujus autem demonstratio pro deperdita est habenda, hujusmodi numeros $aa+1$ alios divisores non admittere, nisi qui ipsi sint summae duorum quadratorum. Quare si numerus in hac forma $aa+1$ contentus habeat divisores, certo scio, hos divisores singulos in forma $pp+qq$ esse contentos. Cum deinde omnes numeri primi formae $4n+1$ sint summae duorum quadratorum, numerorum autem primorum formae $4n-1$ nullus sit duorum quadratorum summa, nullus certe numerus formae $4n-1$ erit divisor formae $aa+1$; sed si ea habeat divisores primos, eos in hac forma $4n+1$ contineri necesse est. Consideravi itaque omnes numeros primos formae $4n+1$, et ea quadrata primum investigavi, quae unitate aucta essent per quemvis horum numerorum primorum divisibilia, quo pacto omnes numeros formae $aa+1$ sum adeptus, qui non sunt numeri primi, reliquos ergo necessario primos esse oportet. Primum autem manifestum est, per binarium, qui est etiam summa duorum quadratorum, formam $aa+1$ esse divisibilem, quoties a fuerit numerus impar. Superest ergo, ut ii ipsius a valores indagentur, qui reddant formam $aa+1$ divisibilem per quemquam horum numerorum primorum 5, 13, 17, 29, 37, 41, etc. qui ipsi sunt duorum quadratorum summae; quem in finem praemitto sequens problema:

Problema 1. Proposito numero primo formae $4n + 1$, invenire omnia quadrata, quae unitate aucta per illum sunt divisibilia.

Solutio. Cum iste numerus primus sit summa duorum quadratorum, sit $4n + 1 = pp + qq$, quadratum vero unitate auctum per illum divisibile sit $aa + 1$. Demonstravi autem, quando summa duorum quadratorum, veluti $aa + bb$, divisibilis est per numerum primum $pp + qq$, semper dari duos hujusmodi numeros r et s, ut sit $a = pr + qs$ et $b = ps - qr$ (*). Nostro casu ergo cum sit $bb = 1$, necesse est, ut sit $ps - qr = \pm 1$: unde perspicitur fractiones $\frac{p}{q}$ et $\frac{r}{s}$ proxime inter se convenire, ita ut earum differentia $\frac{ps - qr}{qs}$ minorem numeratorem, unitate quippe aequalem, habere nequeat. Quare cum numeri p et q ex aequalitate $4n + 1 = pp + qq$ sint cogniti, formetur fractio $\frac{p}{q}$, quaeraturque in numeris minoribus fractio $\frac{r}{s}$ illi proxime aequalis, ut partibus per crucem multiplicatis productorum ps et qr differentia sit $= 1$, id quod methodo a me alibi exposita facile fiet (**); tum ad fractionem $\frac{p}{q}$ inventa hac fractione $\frac{r}{s}$, erit quadrati unius quaesiti radix $a = pr + qs$, vel etiam $a = -pr - qs$. Tum vero si multiplum quodcunque divisoris $4n + 1$ addatur, habebitur quoque valor idoneus pro a. Generatim ergo erit $a = m(4n + 1) \pm (pr + qs)$, in qua forma continentur radices omnium quadratorum, quae unitate aucta per numerum primum propositum $4n + 1$ sunt divisibilia. Q. E. I.

Scholion. Quemadmodum autem data fractione $\frac{p}{q}$ aliam fractionem $\frac{r}{s}$ inveniri conveniat, quae ab illa tam parum discrepet, ut producta per crucem orta ps et qr unitate tantum differant, alio loco ostendi (***). Scilicet pro numeris p et q eadem operatio institui debet, quae vulgo ad eorum maximum communem divisorem inveniendum institui solet, tum ex quotis ordine scriptis formentur fractiones, quales ex fractionibus continuis prodeunt, earumque ultima erit ipsa fractio $\frac{p}{q}$, penultima autem pro $\frac{r}{s}$ assumi poterit, eritque differentia inter producta ps et qr unitati aequalis; propterea quod numeri p et q erunt inter se primi, quoniam alias numerus $4n + 1 = pp + qq$ non foret primus. Inventa autem fractione $\frac{r}{s}$, manifestum est, ejus loco quoque assumi posse has fractiones $\frac{p + r}{q + s}$, $\frac{2p + r}{2q + s}$ et in genere $\frac{mp + r}{mq + s}$, nam et haec fractio cum fractione $\frac{p}{q}$ comparata dat producta per crucem $mpq + qr$ et $mpq + ps$ unitate differentia. Quod si autem fractioni $\frac{p}{q}$ haec $\frac{mp + r}{mq + s}$ adjungatur, ex iis pro radice quadrati quaesiti obtinetur

$$a = mpp + pr + mqq + qs = m(4n + 1) + pr + qs \quad \text{ob} \quad pp + qq = 4n + 1.$$

Seu cum numeri r et s quoque negative accipi queant, $a = m(4n + 1) \pm (pr + qs)$, quae est ipsa forma generalis in solutione inventa. Verum haec operatio commodissime per exempla docebitur.

Exemplum 1. *Invenire omnia quadrata, quae unitate aucta sint per numerum primum* 29 *divisibilia.*

Sit a radix quadrata ex quadratis quaesitis, et cum 29 sit numerus primus formae $4n + 1$, erit certe summa duorum quadratorum, quae sunt 25 et 4, ita ut ob $29 = pp + qq = 5^2 + 2^2$, sit $p = 5$ et $q = 2$, unde formatur ista fractio $\frac{p}{q} = \frac{5}{2}$. Nunc inter numeros 5 et 2 instituatur operatio ad maximum communem divisorem investigandum, quae ita se habebit:

(*) V. pag. 158, § 8. (**) V. Nov. Comment. T XI pag. 53. (***) V. l. c.

```
2) 5 (2
   4
   —
   1) 2 (2
      2
      —
      0
```

Sunt ergo quoti 2 et 2, ex quibus formantur fractiones sequenti modo:

$$\begin{matrix} & 2 & 2 & \\ \frac{1}{0}, & & \frac{2}{1}, & \frac{5}{2} \end{matrix}$$

eritque penultima $\frac{2}{1} = \frac{r}{s}$, ex his autem duabus ultimis fractionibus $\frac{2}{1}$ et $\frac{5}{2}$ valor idoneus pro a erit productum numeratorum $2.5 = 10$, auctum producto denominatorum $1.2 = 2$; unde erit $a = 10 + 2 = 12$, et in genere $a = 29m \pm 12$; omniumque horum numerorum quadrata unitate aucta per 29 erunt divisibilia. Quare omnes valores ipsius a in his duabus progressionibus arithmeticis continebuntur:

12, 41, 70, 99, 128, 157, 186, 215, 244, 273, etc.
17, 46, 75, 104, 133, 162, 191, 220, 249, 278, etc.

Exemplum 2. *Invenire omnia quadrata, quae unitate aucta fiant per numerum primum* 617 *divisibilia.*

Cum sit $617 = 16^2 + 19^2$, statuatur $p = 19$ et $q = 16$, fiatque inter numeros 16 et 19 haec operatio:

```
16) 19 (1
    16
    —
    3) 16 (5
       15
       —
       1) 3 (3
          3
          —
          0
```

Ex quotis 1, 5, 3 sequentes formentur fractiones:

$$\begin{matrix} & 1 & 5 & 3 & \\ \frac{1}{0}, & & \frac{1}{1}, & \frac{6}{5}, & \frac{19}{16} \end{matrix}$$

quarum binae postremae dant numeratorum productum $= 114$
.... at denominatorum productum $= 80$
unde idoneus isque minimus valor ipsius a erit $= 194$

et generatim $a = 617m \pm 194$. Omnes ergo ipsius a valores in duabus sequentibus progressionibus arithmeticis comprehenduntur:

194, 811, 1428, 2045, 2662, 3279 etc.
423, 1040, 1657, 2274, 2891, 3508 etc.

Exemplum 3. *Invenire omnia quadrata, quae unitate aucta sint per numerum primum* 1709 *divisibilia.*

Cum sit $1709 = 22^2 + 35^2$, inter numeros 22 et 35 sequens instituatur operatio:

$$\begin{array}{l}
22)\ 35\ (1 \\
\quad\ \ 22 \\
\quad\ \ \overline{13)\ 22\ (1} \\
\qquad\quad\ 13 \\
\qquad\quad\ \overline{9)\ 13\ (1} \\
\qquad\qquad\ \ 9 \\
\qquad\qquad\ \overline{4)\ 9\ (2} \\
\qquad\qquad\quad\ \ 8 \\
\qquad\qquad\quad\ \overline{1)\ 4\ (4} \\
\qquad\qquad\qquad\ 4 \\
\qquad\qquad\qquad\ \overline{0}
\end{array}$$

et ex quotis 1, 1, 1, 2, 4 formentur sequentes fractiones:

$$\begin{array}{cccccc}
1 & 1 & 1 & 2 & 4 & \\
\frac{1}{0}, & \frac{1}{1}, & \frac{2}{1}, & \frac{3}{2}, & \frac{8}{5}, & \frac{35}{22}
\end{array}$$

quarum duae ultimae dabunt pro uno ipsius a valore:

$$a = 8.35 + 5.22 = 390$$

ita ut omnes ipsius a valores satisfacientes sint:

$$a = 1709m \pm 390.$$

Coroll. 1. Si numerus primus $4n + 1$ fuerit ipse quadratum unitate auctum, veluti

$$4n + 1 = p^2 + 1,$$

tum ob $q = 1$, sequens operatio erit instituenda:

$$\begin{array}{l}
1)\ p\ (p \\
\quad\ \ p \\
\quad\ \ \overline{0}
\end{array}$$

unicus ergo habetur quotus p, ex quo nascentur fractiones

$$\begin{array}{cc}
p & \\
\frac{1}{0}, & \frac{p}{1}
\end{array}$$

unde fit $a = 1.p + 0.1 = p$, et generatim $a = m(4n + 1) \pm p$.

Coroll. 2. Si amborum quadratorum, quorum summae numerus primus $4n + 1$ aequatur, radices unitate differant ut sit $4n + 1 = pp + (p - 1)^2$, tum ob $q = p - 1$, sequens habebitur operatio:

$$\begin{array}{l} p-1)\; p \;\; (1 \\ \quad\quad\;\; \underline{p-1} \\ \quad\quad\quad\;\; 1)\; p-1\; (p-1 \\ \quad\quad\quad\quad\;\;\; \underline{p-1} \\ \quad\quad\quad\quad\quad\;\;\; 0 \end{array}$$

Quoti ergo 1 et $p-1$ has dabunt fractiones:

$$\begin{array}{ccc} & 1 & p-1 \\ \frac{1}{0}, & \frac{1}{1}, & \frac{p}{p-1} \end{array}$$

unde fit $a = 1.p + 1.(p-1) = 2p-1$, et in genere $a = (4n+1)m \pm (2p-1)$.

Coroll. 3. Si quaerantur omnia quadrata, quae unitate aucta sint per numerum primum $2 = 1 + 1$ divisibilia, etsi 2 non est formae $4n+1$, tamen, quia $p = 1$ et $q = 1$, erit primo $a = 1$ per coroll. 1, hincque in genere $a = 2m \pm 1$. Unde sequitur, quod per se est manifestum, omnia quadrata numerorum imparium, si unitas addatur, fore per 2 divisibilia.

Scholion 2. Secundum hanc ergo regulam omnes numeros primos formae $4n+1$ tractavi, et postquam singulos in summam duorum quadratorum converti, quod semper et quidem unico modo fieri potest, cuique formam generalem ipsius a, in qua radices omnium quadratorum, quae unitate aucta per quemque numerum primum sint divisibilia, adscripsi, unde sequens nata est tabula:

Tabula omnium numerorum a,

quorum quadrata, unitate aucta, $aa+1$, sunt per quemlibet numerum primum formae $4n+1$ divisibilia.

Numeri primi	Valor ipsius a
$2 = 1^2 + 1^2$	$a = 2m \pm 1$
$5 = 1^2 + 2^2$	$a = 5m \pm 2$
$13 = 2^2 + 3^2$	$a = 13m \pm 5$
$17 = 1^2 + 4^2$	$a = 17m \pm 4$
$29 = 2^2 + 5^2$	$a = 29m \pm 12$
$37 = 1^2 + 6^2$	$a = 37m \pm 6$
$41 = 4^2 + 5^2$	$a = 41m \pm 9$
$53 = 2^2 + 7^2$	$a = 53m \pm 23$
$61 = 5^2 + 6^2$	$a = 61m \pm 11$
$73 = 3^2 + 8^2$	$a = 73m \pm 27$
$89 = 5^2 + 8^2$	$a = 89m \pm 34$
$97 = 4^2 + 9^2$	$a = 97m \pm 22$
$101 = 1^2 + 10^2$	$a = 101m \pm 10$
$109 = 3^2 + 10^2$	$a = 109m \pm 33$
$113 = 7^2 + 8^2$	$a = 113m \pm 15$
$137 = 4^2 + 11^2$	$a = 137m \pm 37$
$149 = 7^2 + 10^2$	$a = 149m \pm 44$
$157 = 6^2 + 11^2$	$a = 157m \pm 28$
$173 = 2^2 + 13^2$	$a = 173m \pm 80$
$181 = 9^2 + 10^2$	$a = 181m \pm 19$
$193 = 7^2 + 12^2$	$a = 193m \pm 81$
$197 = 1^2 + 14^2$	$a = 197m \pm 14$
$229 = 2^2 + 15^2$	$a = 229m \pm 107$
$233 = 8^2 + 13^2$	$a = 233m \pm 89$
$241 = 4^2 + 15^2$	$a = 241m \pm 64$
$257 = 1^2 + 16^2$	$a = 257m \pm 16$
$269 = 10^2 + 13^2$	$a = 269m \pm 82$
$277 = 9^2 + 14^2$	$a = 277m \pm 60$
$281 = 5^2 + 16^2$	$a = 281m \pm 53$
$293 = 2^2 + 17^2$	$a = 293m \pm 138$
$313 = 12^2 + 13^2$	$a = 313m \pm 25$
$317 = 11^2 + 14^2$	$a = 317m \pm 114$

Numeri primi	Valor ipsius a
$337 = 9^2 + 16^2$	$a = 337m \pm 148$
$349 = 5^2 + 18^2$	$a = 349m \pm 136$
$353 = 8^2 + 17^2$	$a = 353m \pm 42$
$373 = 7^2 + 18^2$	$a = 373m \pm 104$
$389 = 10^2 + 17^2$	$a = 389m \pm 115$
$397 = 6^2 + 19^2$	$a = 397m \pm 63$
$401 = 1^2 + 20^2$	$a = 401m \pm 20$
$409 = 3^2 + 20^2$	$a = 409m \pm 143$
$421 = 14^2 + 15^2$	$a = 421m \pm 29$
$433 = 12^2 + 17^2$	$a = 433m \pm 179$
$449 = 7^2 + 20^2$	$a = 449m \pm 67$
$457 = 4^2 + 21^2$	$a = 457m \pm 109$
$461 = 10^2 + 19^2$	$a = 461m \pm 48$
$509 = 5^2 + 22^2$	$a = 509m \pm 208$
$521 = 11^2 + 20^2$	$a = 521m \pm 235$
$541 = 10^2 + 21^2$	$a = 541m \pm 52$
$557 = 14^2 + 19^2$	$a = 557m \pm 118$
$569 = 13^2 + 20^2$	$a = 569m \pm 86$
$577 = 1^2 + 24^2$	$a = 577m \pm 24$
$593 = 8^2 + 23^2$	$a = 593m \pm 77$
$601 = 5^2 + 24^2$	$a = 601m \pm 125$
$613 = 17^2 + 18^2$	$a = 613m \pm 35$
$617 = 16^2 + 19^2$	$a = 617m \pm 194$
$641 = 4^2 + 25^2$	$a = 641m \pm 154$
$653 = 13^2 + 22^2$	$a = 653m \pm 149$
$661 = 6^2 + 25^2$	$a = 661m \pm 106$
$673 = 12^2 + 23^2$	$a = 673m \pm 58$
$677 = 1^2 + 26^2$	$a = 677m \pm 26$
$701 = 5^2 + 26^2$	$a = 701m \pm 135$
$709 = 15^2 + 22^2$	$a = 709m \pm 96$
$733 = 2^2 + 27^2$	$a = 733m \pm 353$
$757 = 9^2 + 26^2$	$a = 757m \pm 87$
$761 = 19^2 + 20^2$	$a = 761m \pm 39$
$769 = 12^2 + 25^2$	$a = 769m \pm 62$
$773 = 17^2 + 22^2$	$a = 773m \pm 317$
$797 = 11^2 + 26^2$	$a = 797m \pm 215$
$809 = 5^2 + 28^2$	$a = 809m \pm 318$
$821 = 14^2 + 25^2$	$a = 821m \pm 295$
$829 = 10^2 + 27^2$	$a = 829m \pm 246$
$853 = 18^2 + 23^2$	$a = 853m \pm 333$
$857 = 4^2 + 29^2$	$a = 857m \pm 207$
$877 = 6^2 + 29^2$	$a = 877m \pm 151$
$881 = 16^2 + 25^2$	$a = 881m \pm 387$
$929 = 20^2 + 23^2$	$a = 929m \pm 324$
$937 = 19^2 + 24^2$	$a = 937m \pm 196$
$941 = 10^2 + 29^2$	$a = 941m \pm 97$
$953 = 13^2 + 28^2$	$a = 953m \pm 442$
$977 = 4^2 + 31^2$	$a = 977m \pm 252$
$997 = 6^2 + 31^2$	$a = 997m \pm 161$
$1009 = 15^2 + 28^2$	$a = 1009m \pm 469$
$1013 = 22^2 + 23^2$	$a = 1013m \pm 45$
$1021 = 11^2 + 30^2$	$a = 1021m \pm 255$
$1033 = 3^2 + 32^2$	$a = 1033m \pm 347$
$1049 = 5^2 + 32^2$	$a = 1049m \pm 426$
$1061 = 10^2 + 31^2$	$a = 1061m \pm 103$
$1069 = 13^2 + 30^2$	$a = 1069m \pm 249$
$1093 = 2^2 + 33^2$	$a = 1093m \pm 530$
$1097 = 16^2 + 29^2$	$a = 1097m \pm 341$
$1109 = 22^2 + 25^2$	$a = 1109m \pm 354$
$1117 = 21^2 + 26^2$	$a = 1117m \pm 214$
$1129 = 20^2 + 27^2$	$a = 1129m \pm 168$
$1153 = 8^2 + 33^2$	$a = 1153m \pm 140$
$1181 = 5^2 + 34^2$	$a = 1181m \pm 243$
$1193 = 13^2 + 32^2$	$a = 1193m \pm 186$
$1201 = 24^2 + 25^2$	$a = 1201m \pm 49$
$1213 = 22^2 + 27^2$	$a = 1213m \pm 495$
$1217 = 16^2 + 31^2$	$a = 1217m \pm 78$
$1229 = 2^2 + 35^2$	$a = 1229m \pm 597$
$1237 = 9^2 + 34^2$	$a = 1237m \pm 546$
$1249 = 15^2 + 32^2$	$a = 1249m \pm 585$
$1277 = 11^2 + 34^2$	$a = 1277m \pm 113$
$1289 = 8^2 + 35^2$	$a = 1289m \pm 479$
$1297 = 1^2 + 36^2$	$a = 1297m \pm 36$
$1301 = 25^2 + 26^2$	$a = 1301m \pm 51$
$1321 = 5^2 + 36^2$	$a = 1321m \pm 257$
$1361 = 20^2 + 31^2$	$a = 1361m \pm 614$

Numeri primi	Valor ipsius a	Numeri primi	Valor ipsius a
$1373 = 2^2 + 37^2$	$a = 1373m \pm 668$	$1697 = 4^2 + 41^2$	$a = 1697m \pm 414$
$1381 = 15^2 + 33^2$	$a = 1381m \pm 366$	$1709 = 22^2 + 35^2$	$a = 1709m \pm 390$
$1409 = 25^2 + 28^2$	$a = 1409m \pm 452$	$1721 = 11^2 + 40^2$	$a = 1721m \pm 473$
$1429 = 23^2 + 30^2$	$a = 1429m \pm 620$	$1733 = 17^2 + 38^2$	$a = 1733m \pm 410$
$1433 = 8^2 + 37^2$	$a = 1433m \pm 542$	$1741 = 29^2 + 30^2$	$a = 1741m \pm 59$
$1453 = 3^2 + 38^2$	$a = 1453m \pm 497$	$1753 = 27^2 + 32^2$	$a = 1753m \pm 713$
$1481 = 16^2 + 35^2$	$a = 1481m \pm 465$	$1777 = 16^2 + 39^2$	$a = 1777m \pm 775$
$1489 = 20^2 + 33^2$	$a = 1489m \pm 225$	$1789 = 5^2 + 42^2$	$a = 1789m \pm 724$
$1493 = 7^2 + 38^2$	$a = 1493m \pm 432$	$1801 = 24^2 + 35^2$	$a = 1801m \pm 824$
$1549 = 18^2 + 35^2$	$a = 1549m \pm 88$	$1861 = 30^2 + 21^2$	$a = 1861m \pm 61$
$1553 = 23^2 + 32^2$	$a = 1553m \pm 339$	$1873 = 28^2 + 33^2$	$a = 1873m \pm 737$
$1597 = 21^2 + 34^2$	$a = 1597m \pm 610$	$1877 = 14^2 + 41^2$	$a = 1877m \pm 137$
$1601 = 1^2 + 40^2$	$a = 1601m \pm 40$	$1889 = 17^2 + 40^2$	$a = 1889m \pm 331$
$1609 = 3^2 + 40^2$	$a = 1609m \pm 523$	$1901 = 26^2 + 35^2$	$a = 1901m \pm 218$
$1613 = 13^2 + 38^2$	$a = 1613m \pm 127$	$1913 = 8^2 + 43^2$	$a = 1913m \pm 712$
$1621 = 10^2 + 39^2$	$a = 1621m \pm 166$	$1933 = 13^2 + 42^2$	$a = 1933m \pm 598$
$1637 = 26^2 + 31^2$	$a = 1637m \pm 316$	$1949 = 10^2 + 43^2$	$a = 1949m \pm 589$
$1657 = 19^2 + 36^2$	$a = 1657m \pm 783$	$1973 = 23^2 + 38^2$	$a = 1973m \pm 259$
$1669 = 15^2 + 38^2$	$a = 1669m \pm 220$	$1993 = 12^2 + 43^2$	$a = 1993m \pm 834$
$1693 = 18^2 + 37^2$	$a = 1693m \pm 92$	$1997 = 29^2 + 34^2$	$a = 1997m \pm 412$

Tabula ergo haec in se complectitur omnes numeros primos formae $4n + 1$ infra 2000 existentes, ejusque ergo ope omnes numeri inveniri possunt, quorum quadrata unitate aucta per ullum horum numerorum primorum sint divisibilia. Ejus ergo beneficio sequens solvi poterit problema:

Problema. Omnium numerorum, qui unitate excedunt numeros quadratos, assignare omnes divisores radicibus ipsorum quadratis minores.

Solutio. Scribantur ordine omnes numeri ab unitate ad 2000, quandoquidem praecedens tabula ad hunc terminum est producta, qui littera a designentur, ita pro quovis numero inde nato $aa + 1$ divisores sint assignandi. Constat autem, hos numeros alios non esse habituros divisores primos, nisi formae $4n + 1$; praecedens vero tabula omnes numeros a exhibet, quorum quadrata, unitate aucta, sint per quemque numerum primum hujus formae divisibilia. Verum pro quolibet numero $aa + 1$ sufficit notasse divisores primos radice a minores: quoniam his cognitis etiam divisores radice a majores sponte innotescunt. Quamobrem singulis numeris a formae $2m \pm 1$ adscribatur binarius: quia eorum quadrata, unitate aucta, sunt per 2 divisibilia; tum numeris $a = 5m \pm 2$ adscribatur 5, numeris $a = 13m \pm 5$ adscribatur 13, numeris $a = 17m \pm 4$ adscribatur 17, et ita porro: ubi quidem valores ipsius a minores ipso numero primo proposito omittuntur, quia tantum de divisoribus ipso numero a minoribus quaeritur. Hoc ergo modo si ope tabulae praecedentis

cuique numero a divisores convenientes adscribantur, obtinebuntur omnes divisores numeri $aa+1$ ipsa radice a minores. Q. E. I.

Coroll. 1. Si ergo hoc modo numeri a relinquentur, quibus nullus divisor fuerit adscriptus, hoc indicio erit, numeros $aa+1$ inde natos esse primos, nullos quippe divisores admittentes praeter unitatem et se ipsos. Quibus igitur numeris a in tabula hoc modo condita nullus divisor fuerit adscriptus, de iis certo affirmare poterimus, eorum quadrata, unitate aucta, esse numeros primos.

Coroll. 2. Quoniam igitur haec tabula pro numeris a facile ad 2000 extenditur, numeri inde nati $aa+1$ ad 4000000 exsurgent; unde ista tabula omnes numeros primos formae $aa+1$ exhibebit, qui 4 milliones non superant, sicque ex ea numeri primi non solum centenis millibus sed etiam uno millione majores depromi poterunt.

Coroll. 3. Quibus autem numeris a unicus divisor α fuerit adscriptus, numeri inde nati $aa+1$ praeter unitatem unicum habebunt hunc divisorem α, radice a minorem; ideoque $\frac{aa+1}{\alpha}$ erit numerus primus. Ita quibus numeris a solus binarius fuerit adscriptus, ex iis certo hos obtinemus numeros primos $\frac{aa+1}{2}$; atque adeo ex ista tabula omnes numeri primi formae $\frac{aa+1}{2}$ limite 2000000 non majores assignari poterunt.

Coroll. 4. Simili modo omnes numeri a, quibus solus quinarius est adscriptus, praebebunt omnes numeros primos formae $\frac{aa+1}{5}$, qui infra limitem 800000 continentur. Atque omnes numeri a, qui tantum divisorem 13 habebunt adscriptum, praebebunt omnes numeros primos formae $\frac{aa+1}{13}$, infra limitem 307692 contentos.

Coroll. 5. Qui autem numeri a duos tantum divisores α et β habebunt adscriptos, id indicio erit, numeros $\frac{aa+1}{\alpha\beta}$ fore primos. Hinc quibus numeris a tantum duo divisores 2 et 5 fuerint adscripti, ex iis reperientur omnes numeri primi formae $\frac{aa+1}{10}$, qui quidem limitem 400000 non superabunt.

Scholion 1. Verum ut hae conclusiones sint certae, probe notandum est, inter numeros $aa+1$, qui sunt per numerum primum $4n+1$ divisibiles, etiam ejusmodi numeros contineri, qui sint per quadratum $(4n+1)^2$, vel etiam per cubum $(4n+1)^3$, altioresve potestates $(4n+1)^4$, $(4n+1)^5$ etc. divisibiles. Quod quoties accidit, numero a non solum divisor $4n+1$, sed ejus summa potestas, per quam numerus $aa+1$ fuerit divisibilis, adscribi debebit, ut hoc modo omnes divisores primi numerorum $aa+1$, ipsa radice a minores obtineantur. Si quidem divisor fuerit $=2$, nulla ejus altior potestas, veluti 4, 8, 16 etc. unquam numeri $aa+1$ divisor esse poterit, id quod per se est manifestum, cum existente a numero impari, forma $aa+1$ sit numerus impariter par. At de numeris primis formae $4n+1$ dantur utique ejusmodi quadrata, quae unitate aucta sint per quamvis eorum potestatem divisibilia, quos idcirco investigari conveniet.

Scholion 2. Cum autem sit $4n+1=pp+qq$, erunt omnes quoque ipsius $4n+1$ potestates summae duorum quadratorum, et quidem pluribus modis, ex quibus vero id quadratorum par sumi conveniet, quorum radices sunt numeri primi inter se. Sic cum sit in genere

$$(pp + qq)(rr + ss) = (pr + qs)^2 + (ps - qr)^2, \quad \text{erit}$$
$$(4n + 1)^2 = (pp + qq)^2 = 4ppqq + (pp - qq)^2$$
$$(4n + 1)^3 = (pp + qq)^3 = (p^3 - 3pqq)^2 + (3ppq - q^3)^2,$$
$$(4n + 1)^4 = (pp + qq)^4 = (p^4 - 6ppqq + q^4)^2 + (4p^3q - 4pq^3)^2.$$

Si simili modo, quo ante, valores ipsius a investigentur, conficietur pro potestatibus numerorum primorum, quae infra terminum 2000 continentur, sequens tabula:

Tabula omnium numerorum a,

quorum quadrata, unitate aucta, $aa + 1$, sint per potestates numerorum primorum $4n + 1$ divisibilia.

Potestates numerorum primorum	Valor ipsius a
$5^2 = 3^2 + 4^2$	$a = 25\,m \pm 7$
$5^3 = 2^2 + 11^2$	$a = 125\,m \pm 57$
$5^4 = 7^2 + 24^2$	$a = 625\,m \pm 182$
$5^5 = 38^2 + 41^2$	$a = 3125\,m \pm 1068$
$13^2 = 5^2 + 12^2$	$a = 169\,m \pm 70$
$13^3 = 9^2 + 46^2$	$a = 2197\,m \pm 239$
$13^4 = 119^2 + 120^2$	$a = 13^4 m \pm 239$
$17^2 = 8^2 + 15^2$	$a = 289\,m \pm 38$
$17^3 = 47^2 + 52^2$	$a = 17^3 m \pm 1985$
$29^2 = 20^2 + 21^2$	$a = 841\,m \pm 41$
$37^2 = 12^2 + 35^2$	$a = 1369\,m \pm 117$
$41^2 = 9^2 + 40^2$	$a = 1681\,m \pm 378$
$53^2 = 28^2 + 45^2$	$a = 53^2 m \pm 500$
$61^2 = 11^2 + 60^2$	$a = 61^2 m \pm 682$
$73^2 = 48^2 + 55^2$	$a = 73^2 m \pm 776$
$89^2 = 39^2 + 80^2$	$a = 89^2 m \pm 3861$
$97^2 = 65^2 + 72^2$	$a = 97^2 m \pm 4052$
$101^2 = 20^2 + 99^2$	$a = 101^2 m \pm 515$
$109^2 = 60^2 + 91^2$	$a = 109^2 m \pm 5744$
$113^2 = 15^2 + 112^2$	$a = 113^2 m \pm 1710$
$137^2 = 88^2 + 105^2$	$a = 137^2 m \pm 6613$
$149^2 = 51^2 + 140^2$	$a = 149^2 m \pm 1744$
$197^2 = 28^2 + 95^2$	$a = 197^2 m \pm 1393$
$257^2 = 32^2 + 255^2$	$a = 257^2 m \pm 2072$

His itaque subsidiis hic subjunctam construxi tabulam, ex qua statim pro singulis numeris a omnes divisores formae $aa + 1$ habentur. Hanc quidem tabulam non ultra 1500 in radicibus continuavi, sed ope harum formularum facile ad 2000 usque progredi licebit.

Ex hac autem tabula jam plures numeri primi formae $aa+1$ desumi poterunt, qui non solum centenis millibus, sed etiam uno millione sint majores: deinde etiam numeri primi formae $\frac{aa+1}{2}$ et $\frac{aa+1}{5}$, item $\frac{aa+1}{10}$, quos in sequentibus tabellis exhibebo.

Numeri primi formae $aa+1$.

Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$
1	2	176	30977	440	193601	760	577601
2	5	180	32401	444	197137	764	583697
4	17	184	33857	464	215297	780	608401
6	37	204	41617	466	217157	784	614657
10	101	206	42437	470	220901	816	665857
14	197	210	44101	474	224677	826	682277
16	257	224	50177	490	240101	860	739601
20	401	230	52901	496	246017	864	746497
24	577	236	55697	536	287297	890	792101
26	677	240	57601	544	295937	906	820837
36	1297	250	62501	556	309137	910	828101
40	1601	256	65537	570	324901	920	846401
54	2917	260	67601	576	331777	930	864901
56	3137	264	69697	584	341057	936	876097
66	4357	270	72901	594	352837	946	894917
74	5477	280	78401	634	401957	950	902501
84	7057	284	80657	636	404497	960	921601
90	8101	300	90001	644	414737	966	933157
94	8837	306	93637	646	417317	986	972197
110	12101	314	98597	654	427717	1004	1008017
116	13457	326	106277	674	454277	1010	1020101
120	14401	340	115601	680	462401	1036	1073297
124	15377	350	122501	686	470597	1054	1110917
126	15877	384	147457	690	476101	1060	1123601
130	16901	386	148997	696	484417	1066	1136357
134	17957	396	156817	700	490001	1070	1144901
146	21317	400	160001	704	495617	1094	1196837
150	22501	406	164837	714	509797	1096	1201217
156	24337	420	176401	716	512657	1106	1223237
160	25601	430	184901	740	547601	1124	1263377
170	28901	436	190097	750	562501	1140	1299601

Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$	Radices a	Numeri primi $aa+1$
1144	1308737	1246	1552517	1340	1795601	1420	2016401
1146	1313317	1274	1623077	1350	1822501	1430	2044901
1150	1322501	1276	1628177	1354	1833317	1434	2056351
1156	1336337	1290	1664101	1366	1865957	1440	2073601
1174	1378277	1294	1674437	1374	1887877	1456	2119937
1176	1382977	1306	1705637	1376	1893377	1460	2131601
1184	1401857	1314	1726597	1394	1943237	1494	2232037
1210	1464101	1316	1731857	1406	1976837		
1234	1522757	1320	1747401	1410	1988101		
1244	1547537	1324	1752977	1416	2005057		

Habentur ergo hic 112 numeri primi majores quam 100000, et 49 numeri primi millionem superantes.

Praeterea autem plures numeri primi formarum $\frac{aa+1}{2}$, $\frac{aa+1}{5}$, $\frac{aa+1}{10}$ assignari possunt, qui etiam centena millia superant; ut ex sequentibus perspicere licet.

Valores numeri a, quibus forma $\frac{aa+1}{2}$ fit numerus primus.

1, 3, 5, 9, 11, 15, 19, 25, 29, 35, 39, 45, 49, 51, 59, 61, 65, 69, 71, 79, 85, 95
101, 121, 131, 139, 141, 145, 159, 165, 169, 171, 175, 181, 195, 299
201, 205, 209, 219, 221, 231, 245, 261, 271, 275, 279, 289, 199
309, 315, 321, 325, 329, 335, 345, 349, 371, 375, 379, 391, 399
405, 409, 415, 425, 435, 441, 445, 449, 451, 459, 461, 471
519, 521, 529, 535, 545, 559, 569, 571, 575, 579, 581, 595
609, 631, 639, 641, 649, 661, 669, 685, 689, 695, 699
711, 715, 739, 745, 751, 779, 781, 791, 799
815, 819, 821, 841, 855, 861, 869, 875, 881, 885
901, 909, 921, 925, 929, 935, 949, 951, 955, 959, 979, 981, 985, 989, 991
1001, 1011, 1025, 1029, 1031, 1039, 1051, 1055, 1069, 1081, 1091, 1095, 1099
1111, 1125, 1129, 1151, 1155, 1161, 1171, 1179, 1181, 1185, 1199
1205, 1219, 1225, 1241, 1251, 1255, 1265, 1281, 1285, 1299
1311, 1315, 1329, 1345, 1149, 1359, 1361, 1389, 1391
1405, 1411, 1419, 1421, 1439, 1459, 1465, 1469, 1489, 1495, 1499

Valores numeri a, quibus forma $\frac{aa+1}{5}$ fit numerus primus.

2, 8, 12, 22, 28, 42, 48, 52, 58, 62, 78, 88, 92
102, 108, 152, 158, 178, 188, 198
202, 222, 238, 248, 258, 262, 272, 292, 298
308, 312, 328, 352, 358, 362, 388

402, 422, 428, 458, 462, 478, 488, 492
508, 522, 558, 572, 588
602, 622, 628, 638, 652, 662, 692, 798
702, 728, 738, 758, 792
828, 838, 842, 848, 862, 872, 898
908, 912, 942, 962, 972, 978, 988
1008, 1062, 1072, 1078, 1088
1108, 1112, 1138, 1192
1208, 1238, 1272, 1278, 1298
1312, 1342, 1358, 1372, 1378
1402, 1442, 1452, 1472, 1488, 1498

Valores numeri a, quibus forma $\frac{aa+1}{10}$ fit numerus primus.

3, 7, 13, 17, 23, 27, 33, 37, 53, 63, 67, 77, 87, 97
103, 113, 127, 137, 147, 153, 163, 167, 197
223, 227, 247, 263, 267, 277, 283, 287, 297
303, 323, 347, 363, 367, 373, 383, 397
417, 427, 433, 453
503, 513, 517, 527, 533, 537, 547, 553, 573, 587
617, 627, 637, 653, 673, 677, 683
753, 763, 773, 777, 797
817, 823, 833, 847, 867, 873, 877, 883
913, 917, 923, 927, 933, 937, 947, 953, 963, 997
1047, 1053, 1063, 1073
1103, 1117, 1137, 1147, 1163, 1167, 1173, 1187, 1197
1213, 1233, 1247, 1273
1337, 1367, 1377, 1387, 1397
1413, 1417, 1423, 1447, 1473, 1497

Hinc autem iterum novem numeri primi supra 1000000 obtinentur, ex forma scilicet $\frac{aa+1}{2}$, quando $a > 1414$.

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1	2	10	101	19	2. 181	28	5. 157
2	5	11	2. 61	20	401	29	2. 421
3	2. 5	12	5. 29	21	2. 13. 17	30	17. 53
4	17	13	2. 5. 17	22	5. 97	31	2. 13. 37
5	2. 13	14	197	23	2. 5. 53	32	5^2. 41
6	37	15	2. 113	24	577	33	2. 5. 109
7	2. 5^2	16	257	25	2. 313	34	13. 89
8	5. 13	17	2. 5. 29	26	677	35	2. 613
9	2. 41	18	5^2. 13	27	2. 5. 73	36	1297

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
37	2. 5. 137	82	5^2. 193. 269	127	2. 5	172	5. 61. 97
38	5. 17^2	83	2. 5. 13. 53	128	5. 29. 113	173	2. 5. 41. 73
39	2. 761	84		129	2. 53	174	13. 17. 137
40	1601	85	2	130		175	2
41	2. 29^2	86	13. 569	131	2	176	
42	5. 353	87	2. 5	132	5^2. 17. 41	177	2. 5. 13
43	2. 5^2. 37	88	5	133	1. 5. 29. 61	178	5
44	13. 149	89	2. 17. 233	134		179	2. 37
45	2. 1013	90		135	2. 13	180	
46	29. 73	91	2. 41. 101	136	53	181	2
47	2. 5. 13. 17	92	5	137	2. 5	182	5^4. 53
48	5. 461	93	2. 5^2. 173	138	5. 13	183	2. 5. 17
49	2. 1201	94		139	2	184	
50	41. 61	95	2	140	17	185	2. 109. 157
51	2. 1301	96	13. 709	141	2	186	29
52	5. 541	97	2. 5.	142	5. 37. 109	187	2. 5. 13
53	2. 5. 281	98	5. 17. 113	143	2. 5^2	188	5
54	2917	99	2. 13^2. 29	144	89	189	2. 53
55	2. 17. 89	100	73. 137	145	2	190	13
56	3137	101	2	146		191	2. 3, 17. 29
57	2. 5^3. 13	102	5	147	2. 5	192	5. 73. 101
58	5. 673	103	2. 5.	148	5. 13	193	2. 5^3. 149
59	2. 1741	104	29	149	2. 17	194	61
60	13. 277	105	2. 37	150		195	2
61	2. 1861	106	17	151	2. 13	196	41
62	5. 769	107	2. 5^2	152	5	197	2. 5
63	2. 5. 397	108	5	153	2. 5	198	5
64	17. 241	109	2. 13	154	37	199	2
65	2. 2113	110		155	2. 41	200	13. 17. 181
66	4357	111	2. 61. 101	156		201	2
67	2. 5. 449	112	5. 13	157	2. 5^2. 17. 29	202	5
68	5^3. 37	113	2. 5	158	5	203	2. 5. 13
69	2. 2381	114	41	159	2	204	
70	13^2. 29	115	2. 17	160		205	2
71	2. 2521	116		161	2. 13	206	
72	5. 17. 61	117	2. 5. 37^2	162	5. 29	207	2. 5^2
73	2. 5. 13. 41	118	5^2	163	2. 5	208	5. 17
74		119	2. 73. 97	164	13	209	2
75	2. 29. 97	120		165	2	210	
76	53. 109	121	2	166	17	211	2. 113. 197
77	2. 5. 593	122	5. 13	167	2. 5	212	5. 89. 101
78	5	123	2. 5. 17. 89	168	5^2	213	2. 5. 13
79	2	124		169	2	214	41
80	37. 173	125	2. 13	170		215	2. 29
81	2. 17	126		171	2	216	13. 37. 97

a	Divisores ipsius aa + 1	a	Divisores ipsius aa + 1	a	Divisores ipsius aa + 1	a	Divisores ipsius aa + 1
217	2. 5. 17	262	5	307	2. 5². 13. 29	352	5
218	5²	263	2. 5	308	5	353	2. 5. 17
219	2	264		309	2	354	113
220	29	265	2. 13. 37. 73	310	17	355	2. 61
221	2	266	173	311	2. 137	356	13
222	5	267	2. 5	312	5	357	2. 5²
223	2. 5	268	5². 13². 17	313	2. 5. 97. 101	358	5
224		269	2. 97	314		359	2. 13
225	2. 17	270		315	2	360	29. 41. 109
226	13	271	2	316	61	361	2. 17
227	2. 5	272	5	317	2. 5. 13	362	5
228	5. 37	273	2. 5. 29. 257	318	5³	363	2. 5
229	2. 13	274	193	319	2. 17. 41. 73	364	37
230		275	2	320	13	365	2. 29
231	2	276	17	321	2	366	97
232	5²	277	2. 5	322	5. 89. 233	367	2. 5
233	2. 5. 61. 89	278	5. 13. 29. 41	323	2. 5	368	5²
234	17	279	2	324	113	369	2. 13
235	2. 53	280		325	2	370	17
236		281	2. 13	326		371	2
237	2. 5. 41. 137	282	5²	327	2. 5. 17². 37	372	5. 13
238	5	283	2. 5	328	5	373	2. 5
239	2. 13⁴	284		329	2	374	137
240		285	2. 17	330	13	375	2
241	2. 113	286	157	331	2. 29	376	37
242	5. 13. 17. 53	287	2. 5	332	5²	377	2. 5. 61. 233
243	2. 5²	288	5. 53	333	2. 5. 13	378	5. 17. 41²
244	29	289	2	334	281	379	2
245	2	290	37	335	2	380	197
246	73	291	2. 13	336	17. 29. 229	381	2. 181
247	2. 5	292	5	337	2. 5. 41. 277	382	5². 13
248	5	293	2. 5². 17. 101	338	5. 73. 313	383	2. 5
249	2. 29	294	13. 61. 109	339	2. 37	384	
250		295	2. 53	340		385	2. 13
251	2. 17². 109	296	41	341	2. 53	386	
252	5. 13	297	2. 5	342	5. 149. 157	387	2. 5. 17
253	2. 5. 37. 173	298	5	343	2. 5². 13. 181	388	5
254	149	299	2	344	17	389	2. 29
255	2. 13. 41. 61	300		345	2	390	89
256		301	2. 89	346	13	391	2
257	2. 5²	302	5. 17. 29. 37	347	2. 5	392	5. 73
258	5	303	2. 5	348	5. 53	393	2. 5²
259	2. 17	304	13	349	2	394	29. 53. 101
260		305	2. 193. 241	350		395	2. 13. 17. 353
261	2	306		351	2. 229. 269	396	

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
397	2. 5	442	5. 41	487	2. 5. 37	532	5^2
398	5. 13	443	2. 5^2. 157	488	5	533	2. 5
399	2	444		489	2. 13. 17	534	29
400		445	2	490		535	2
401	2. 37. 41. 53	446	17	491	2. 149	536	
402	5	447	2. 5. 13. 29. 53	492	5	537	2. 5
403	2. 5. 109. 149	448	5. 137. 293	493	2. 5^2	538	5. 13. 61. 73
404	17	449	2	494	277	539	2. 29
405	2	450	13. 37. 421	495	2. 101	540	17^2
406		451	2	496		541	2. 13
407	2. 5^2	452	5. 29	497	2. 5. 17	542	5. 41
408	5. 13^2. 197	453	2. 5	498	5. 193. 257	543	2. 5^2
409	2	454	53	499	2. 13. 61. 157	544	
410	97	455	2. 17	500	53^2. 89	545	2
411	2. 13. 73. 89	456	269	501	2. 41	546	241
412	5. 17	457	3. 5^2	502	5. 13	547	2. 5
413	2. 5. 37	458	5	503	2. 5	548	5. 17
414	101	459	2	504	389	549	2. 37
415	2	460	13. 41. 397	505	2. 29	550	113
416	61	461	2	506	17	551	2. 13
417	2. 5	462	5	507	2. 5^2. 97	552	5. 149. 409
418	5^2. 29. 241	463	2. 5. 13. 17. 97	508	5	553	2. 5
419	2. 41	464		509	2. 281. 461	554	13
420		465	2. 73	510	29	555	2. 233
421	2. 13. 17. 401	466		511	2. 137	556	
422	5	467	2. 5. 113. 193	512	5. 13. 37. 109	557	2. 5^3. 17. 73
423	2. 5. 29	468	5^2	513	2. 5	558	5
424	13	469	2. 109	514	17	559	2
425	2	470		515	2. 13. 101^2	560	61. 97
426	173	471	2	516	449	561	2. 37
427	2. 5	472	5. 17	517	2. 5.	562	5. 181. 349
428	5	473	2. 5. 13	518	5^2	563	2. 5. 29
429	2. 17	474		519	2	564	13
430		475	2. 37	520	317	565	2. 17. 41. 229
431	2. 293. 317	476	13. 29	521	2	566	457
432	5^3	477	2. 5. 61. 373	522	5	567	2. 5. 13
433	2. 5	478	5	523	2. 5. 17	568	5^3. 29. 89
434	13	479	2. 89	524	37. 41. 181	569	2
435	2	480	17	525	2. 13	570	
436		481	2. 29	526	337	571	2
437	2. 5. 13^2. 113	482	5^2	527	2. 5	572	5
438	5. 17. 37. 61	483	2. 5. 41	528	5. 13	573	2. 5
439	2. 173	484	73	529	2	574	17
440		485	2. 337. 349	530	257	575	2
441	2	486	13	531	2. 17	576	

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
577	2. 5. 13^2. 197	622	5	667	2. 5. 17	712	5. 53
578	5. 109	623	2. 5. 37	668	5^2. 13	713	2. 5. 29
579	2	624	41	669	2	714	
580	13. 113. 229	625	2. 17	670	593	715	2
581	2	626	29	671	2. 13	716	
582	5^2. 17	627	2. 5.	672	5. 37	717	2. 5. 101. 509
583	2. 5. 41	628	5	673	2. 5	718	5^2. 17
584		629	2. 13	674		719	2. 53
585	2. 137	630	73	675	2. 409. 557	720	13
586	37	631	2	676	17	721	2. 61
587	2. 5	632	5^2. 13	677	2. 5	722	5. 137
588	5	633	2. 5. 17	678	5. 89	723	2. 5. 13
589	2. 89	634		679	2. 29	724	293
590	13	635	2. 37	680		725	2. 269
591	2. 17	636		681	2. 13	726	601
592	5. 29	637	2. 5	682	5^3. 61^2	727	2. 5. 17
593	2. 5^2. 13. 541	638	5	683	2. 5	728	5
594		639	2	684	13. 17. 29. 73	729	2. 41
595	2	640	149	685	2	730	109
596	101	641	2	686		731	2. 397. 673
597	2. 5. 29	642	5. 13. 17. 373	687	2. 5. 109. 433	732	5^2
598	5. 37	643	2. 5^2	688	5. 41	733	2. 5. 29
599	2. 17. 61. 173	644		689	2	734	37
600	157	645	2. 13	690		735	2. 17
601	2. 313. 577	646		691	2. 193	736	13
602	5	647	2. 5. 41	692	5	737	2. 5. 13
603	2. 5. 13	648	5. 137. 613	693	2. 5^2. 12. 113	738	5
604	97	649	2	694	13	739	2
605	2. 197	650	17. 29	695	2	740	
606	13^2. 41. 53	651	2. 313	696		741	2. 293
607	2. 5^2	652	5	697	2. 5. 13. 37. 101	742	5. 29
608	5. 17	653	2. 5	698	5	743	2. 5^2. 61. 181
609	2	654		699	2	744	17
610	233	655	2. 13. 29. 569	700		745	2
611	2. 73	656	157	701	2. 17. 97. 149	746	13^2. 37. 89
612	5. 173. 433	657	2. 5^2. 89. 97	702	5	747	2. 5. 41
613	2. 5. 53	658	5. 13	703	2. 5. 73. 677	748	5. 317. 353
614	277	659	2. 17. 53. 241	704		749	2. 13
615	2. 281	660	37. 61. 193	705	2. 181	750	
616	13. 17^2. 101	661	2	706	41	751	2
617	2. 5	662	5	707	2. 5^2. 13	752	5. 17
618	5^2	663	2. 5. 113. 389	708	5. 29	753	2. 5
619	2. 13	664	353	709	2. 37	754	97
620	269	665	2. 41	710	13. 17	755	2. 257
621	2. 29. 61. 109	666	53	711	2	756	521

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
757	2. 5^2. 73. 157	802	5. 197. 653	847	2. 5.	892	5. 13
758	5	803	2. 5. 17	848	5	893	2. 5^2. 41. 389
759	2. 13	804	61	849	2. 73	894	37
760		805	2. 457. 709	850	13. 149. 373	895	2. 97
761	2. 17	806	113	851	2. 97	896	281
762	5. 13	807	2. 5^4. 521	852	5. 41	897	2. 5. 17
763	2. 5	808	5. 37	853	2. 5. 13. 29. 193	898	5
764		809	2. 229	854	17	899	2. 101
765	2. 53	810	509	855	2	900	241
766	29	811	2. 13. 41. 617	856	89	901	2
767	2. 5. 89. 661	812	5. 17	857	2. 5^2. 37. 397	902	5. 13
768	5^2	813	2. 5. 157. 421	858	5. 29	903	2. 5. 73
769	2. 17	814	13	859	2. 137	904	61
770	41	815	2	860		905	2. 13. 17^2. 109
771	2. 29. 37. 277	816		861	2	906	
772	5. 13. 53. 173	817	2. 5	862	5	907	2. 5^2
773	2. 5.	818	5^2. 53. 101	863	2. 5. 13. 17. 337.	908	5
774	197	819	2	864		909	2
775	2. 13^2	820	17. 37	865	2. 61	910	
776	73^2. 113	821	2	866	13	911	2. 29. 41. 349
777	2. 5	822	5. 337. 401	867	2. 5	912	5
778	5. 17	823	2. 5	868	5^2	913	2. 5
779	2	824	13. 29	869	2	914	17. 157. 331
780		825	2. 53	870	41	915	2. 13^2
781	2	826		871	2. 17. 53. 421	916	29
782	5^2. 61. 401	827	2. 5. 13	872	5	917	2. 5
783	2. 5. 37	828	5	873	2. 5	918	5^2. 13
784		829	2. 17^2. 29. 41	874	461	919	2. 37. 101. 113
785	2. 13. 137. 173	830	73	875	2	920	
786	17	831	2. 449. 769	876	13	921	2
787	2. 5. 241. 257	832	5^2	877	2. 5	922	5. 17. 73. 137
788	5. 13. 41. 233	833	2. 5	878	5. 53	923	2. 5
789	2. 149	834	349	879	2. 13	924	53. 89. 181
790	281	835	2. 89	880	17	925	2.
791	2	836	701	881	2	926	61
792	5	837	2. 5. 13. 17. 317	882	5^2. 29^2. 37	927	2. 5
793	2. 5^2	838	5	883	2. 5	928	5. 13
794	229	839	2. 109	884	193	929	2
795	2. 17. 29. 641	840	13	885	2	930	
796	109	841	2	886	181	931	2. 13. 17. 37. 53
797	2. 5	842	5	887	2. 5. 29	932	5^3
798	5. 13. 97. 101	843	2. 5^2. 61. 233	888	5. 17	933	2. 5
799	2	844	757	889	2. 13. 113. 269	934	41
800	29^2. 761	845	2. 37	890		935	2
801	2. 13	846	17	891	2. 277	936	

a	Divisores ipsius aa + 1	a	Divisores ipsius aa + 1	a	Divisores ipsius aa + 1	a	Divisores ipsius aa + 1
937	2. 5	982	5². 17	1027	2. 5. 29	1072	5
938	5. 149	983	2. 5. 13	1028	5. 241. 877	1073	2. 5
939	2. 17	984	53	1029	2	1074	13
940	29	985	2	1030	37. 53. 541	1075	2. 17. 41. 829
941	2. 13	986		1031	2	1076	233
942	5	987	2. 5. 61	1032	5². 13. 29. 113	1077	2. 5. 193. 601
943	2. 5³	988	5	1033	2. 5. 17	1078	5
944	13²	989	2	1034	41. 89. 293	1079	2. 37
945	2. 29. 89. 173	990	17	1035	2. 13	1080	773
946		991	2	1036		1081	2
947	2. 5	992	5. 97	1037	2. 5. 53	1082	5²
948	5. 17. 97. 109	993	2. 5². 13. 37. 41	1038	5. 229. 941	1083	2. 5. 53
949	2	994	269	1039	2	1084	13². 17. 409
950		995	2. 73	1040	617	1085	2. 29
951	2	996	13. 137. 557	1041	2. 17	1086	733
952	5. 41	997	2. 5	1042	5. 37	1087	2. 5. 13. 61. 149
953	2. 5	998	5. 29	1043	2. 5²	1088	5
954	13	999	2. 17. 149. 197	1044	257	1089	2. 97
955	2	1000	101	1045	2. 13. 97. 433	1090	29. 53
956	17. 37	1001	2	1046	193	1091	2
957	2. 5². 13	1002	5. 113	1047	2. 5	1092	5. 17
958	5. 173	1003	2. 5. 29	1048	5. 13. 61. 277	1093	2. 5²
959	2	1004		1049	2. 73	1094	
960		1005	2. 37	1050	17	1095	2
961	2. 409	1006	13	1051	2	1096	
962	5	1007	2. 5². 17	1052	5. 389. 569	1097	2. 5. 13
963	2. 5	1008	5	1053	2. 5	1098	5. 41
964	313	1009	2. 13	1054		1099	2
965	2. 17. 61. 449	1010		1055	2	1100	13
966		1011	2	1056	29	1101	2. 17. 101. 353
967	2. 5. 13	1012	5. 257. 797	1057	2. 5³. 41. 109	1102	5. 89
968	5². 37	1013	2. 5. 89	1058	5. 13. 17. 1013	1103	2. 5
969	2. 29	1014	109	1059	2. 137	1104	37
970	13. 157. 461	1015	2. 373	1060		1105	2. 181
971	2. 197	1016	17. 41	1061	2. 13. 29	1106	
972	5	1017	2. 5. 293. 353	1062	5	1107	2. 5²
973	2. 5. 17	1018	5²	1063	2. 5	1108	5
974	29	1019	2. 13	1064	857	1109	2. 17. 61. 593
975	2. 41	1020	101	1065	2. 317	1110	13
976	73	1021	2. 233	1066		1111	2
977	2. 5. 53	1022	5. 13	1067	2. 5. 17. 37. 181	1112	5
978	5	1023	2. 5. 229. 457	1068	5³. 73	1113	2. 5. 13². 733
979	2	1024	17	1069	2	1114	29
980	13	1025	2	1070		1115	2. 113
981	2	1026	61	1071	2. 13. 157. 281	1116	37. 41. 821

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1117	2. 5	1162	5. 13	1207	2. 5^2	1252	5. 37^2. 229
18	5^2. 17^2. 173	63	2. 5	8	5	53	2. 5. 13^2. 929
19	2. 29	64	1061	9	2. 61	54	17. 233. 397
1120	433	65	2. 13	1210		55	2
21	2. 101	66	109	11	2. 17	56	13
22	5. 73	67	2. 5.	12	5. 89	57	2. 5^3
23	2. 5. 13. 89. 109	68	5^2. 197. 277	13	2. 5	58	5. 113
24		69	2. 17	14	13. 73	59	2. 29
25	2	1170	61	15	2. 37	1260	349
26	13. 17	71	2	16	661	61	2. 613
27	2. 5. 157. 809	72	5. 29	17	2. 5. 13	62	5. 17. 41. 457
28	5. 397. 641	73	2. 5	18	5^2	63	2. 5. 269. 593
29	2	74		19	2	64	29. 37
1130	577	75	2. 13	1220	17	65	2
31	2. 173	76		21	2. 41	66	13
32	5^2	77	2. 5. 17. 29. 281	22	5. 101	67	2. 5. 229. 701
33	2. 5. 137. 937	78	5. 13. 37. 577	23	2. 5. 373. 401	68	5^2. 73. 881
34	541	79	2	24	569	69	2. 13. 241. 257
35	2. 17	1180	41	25	2	1270	61. 137. 193
36	13. 53	81	2	26	509	71	2. 17
37	2. 5	82	5^3	27	2. 5. 13. 37. 313	72	5
38	5	83	2. 5. 349. 401	28	5. 17. 113. 157	73	2. 5
39	2. 13. 41	84		29	2. 773. 977	74	
1140		85	2	1230	13. 29	75	2. 109
41	2. 37. 73. 241	86	17. 97. 853	31	2. 61	76	
42	5. 97	87	2. 5	32	5^2. 109. 557	77	2. 5. 313. 521
43	2. 5^2. 17. 29. 53	88	5. 13	33	2. 5	78	5
44		89	2. 53	34		79	2. 13. 17
45	2. 113	1190	37	35	2. 29	1280	41. 89. 449
46		91	2. 13. 89. 613	36	149	81	2
47	2. 5	92	5	37	2. 5. 17	82	5^2. 13^2. 389
48	5. 29. 61. 149	93	2. 5^2	38	5	83	2. 5. 97
49	2. 13	94	17^2	39	2. 41. 97. 193	84	157
1150		95	2. 73	1240	13	85	2
51	2	96	53. 137. 197	41	2	86	181
52	5. 13. 17	97	2. 5	42	5. 53	87	2. 5. 73
53	2. 5. 37	98	5. 41	43	2. 5^2. 13	88	5. 17. 29. 673. 1033
54	317	99	2	44		89	2. 37
55	2	1200	337	45	2. 17	1290	
56		1	2. 13. 29	46		91	2. 173
57	2. 5^2. 41. 653	2	5. 101	47	2. 5	92	5. 13. 61
58	5. 269. 997	3	2. 5. 17	48	5. 181	93	2. 5^2. 29. 1153
59	2. 337	4	13	49	2. 53	94	
1160	17	5	2	1250	1201	95	2. 13. 53. 1217
61	2	6	29	51	2	96	17

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1297	2. 5. 149. 1129	1342	5	1387	2. 5	1432	5^4. 17. 193
98	5	43	2. 5^2.	88	5. 373	33	2. 5. 29. 73. 97
99	2	44	13. 41	89	2	34	
1300	809	45	2	1390	17. 89. 1277	35	2. 13
1	2. 37. 89. 257	46	29	91	2	36	641
*2	5. 53	47	2. 5. 13. 17. 821	92	5. 61	37	2. 5. 37
3	2. 5. 41^2. 101	48	5. 53	93	2. 5^2. 197^2	38	5. 13. 29. 1097
4	173	49	2	94		39	2
5	2. 13. 17	1350		95	2. 953	1440	
6		51	2. 29	96	13	41	2. 17. 157. 389
7	2. 5^3	52	5. 281. 1301	97	2. 5	42	5
8	5. 13	53	2. 5. 61	98	5. 17	43	2. 5^3
9	2. 233	54		99	2. 13	44	41
1310	293	55	2. 53	1400	37	45	2. 277
11	2	56	17	1	2. 53	46	149
12	5	57	2. 5^2. 13	2	5	47	2. 5.
13	2. 5. 17	58	5	3	2. 5. 41	48	5. 13
14		59	2	4	29. 101. 673	49	2. 17. 37
15	2	1360	13. 73	5	2	1450	109
16		61	2	6		51	2. 13^2
17	2. 5. 29	62	5. 41	7	2. 5^2. 17^2. 137	52	5
18	5^3. 13	63	2. 5. 37	8	5. 53	53	2. 5. 61
19	2. 509	64	17	9	2. 13. 29	54	53. 113. 353
1320		65	2. 197	1410		55	2. 653
21	2. 13. 41	66		11	2	56	
22	2. 17. 29. 709	67	2. 5	12	5. 13. 37. 829	57	2. 5^2
23	2. 5. 101	68	5^2	13	2. 5	58	5. 17. 89. 281
24		69	2. 89	14	61. 73. 449	59	2
25	2. 277	1370	13. 353. 409	15	2. 17	1460	
26	37	71	2. 113	16		61	2. 13. 53
27	2. 5. 293. 601	72	5	17	2. 5	62	5. 29
28	5. 521. 677	73	2. 5. 13. 17. 853	18	5^2	63	2. 5. 193. 1109
29	2	74		19	2	64	13. 173. 953
1330	17	75	2. 29. 37. 881	1420		65	2
31	2. 13. 61. 1117	76		21	2	66	17
32	5^2	77	2. 5	22	5. 13^2	67	2. 5. 29. 41. 181
33	2. 5. 137. 1297	78	5	23	2. 5	68	5^2
34	13	79	2. 797. 1193	24	17. 101. 1181	69	2
35	2. 461	1380	29. 97. 677	25	2. 13	1470	137
36	97	81	2. 17	26	41	71	2. 317
37	2. 5.	82	5^2. 241. 317	27	2. 5. 269. 757	72	5
38	5. 37	83	2. 5. 13	28	5. 617. 661	73	2. 5
39	2. 17	84	109	29	2. 181	74	13. 37
1340		85	2. 41. 149. 157	1430		75	2. 17. 61. 1049
41	2. 73. 109. 113	86	13	31	2. 461	76	769

a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$	a	Divisores ipsius $aa+1$
1477	2. 5. 13. 97. 173	1483	2. 5. 17^2. 761	1489	2	1495	2
78	5. 433. 1009	84	113	90	13. 313	96	29. 229. 337
79	2. 89	85	2. 41	91	2. 29	97	2. 5
1480	457	86	37^2	92	5. 17	98	5
81	2. 229	87	2. 5. 13. 73. 233	93	2. 5^2. 109. 409	99	2
82	5^2	88	5	94		1500	13. 17

XXVI.

Quomodo numeri praemagni sint explorandi, utrum sint primi, nec ne.

(N. Comment. XIII. 1768 p. 67. Exhib. 1765. Dec. 19.)

1. Ante omnia monendum est, me hic non ejusmodi methodum polliceri, cujus ope omnes omnino numeri, cujuscunque sint generis, examinari queant, utrum sint primi nec ne? Hujusmodi enim methodum vix aliam dari posse existimo, nisi quae ad regulam redeat vulgarem, qua divisio per omnes numeros primos, radice quadrata numeri propositi minores, est tentanda, quae operatio sane, si numeri saltem mediocriter magni proponantur, nimis est molesta, quam ut suscipi queat. Quae igitur hic in medium afferre constitui; ad certum tantum numerorum genus sunt restringenda, pro quo scilicet hoc examen, utrum sint primi nec ne? citra laborem tam operosum institui queat. Cum enim numerorum primorum natura adhuc maxime sit abscondita, quicquid in hoc negotio praestare licuerit, etiamsi alias arctissimis limitibus sit circumscriptum, usu neutiquam destitui est censendum.

2. Numeros ergo tantum in hac forma $4n+1$ contentos sum contemplaturus, de quibus equidem post Fermatium demonstravi, si hujusmodi numerus fuerit primus, tum eum semper esse summam duorum quadratorum, idque unico modo. Unde proposito numero quocunque hujus formae $4n+1$, examen utrum sit primus nec ne? hoc modo instituetur. Ab eo successive omnes numeri quadrati ipso minores auferantur, eaque notentur residua, quae pariter sint numeri quadrati; atque si unico modo numerus propositus $4n+1$ in forma $aa+bb$ contineri deprehendatur, id certum erit criterium numerum propositum esse primum. Sin autem vel prorsus non in ea forma contineatur, vel plus uno modo, tum certe non erit primus; priori quidem casu, quo numerus $4n+1$ non est summa duorum quadratorum, plus concludere non licet, quam eum non esse primum, neque inde ejus divisores innotescunt, sin autem plus uno modo fuerit duorum quadratorum summa, veluti $4n+1 = aa+bb = cc+dd$, tum hinc quaerantur ejusmodi bini numeri p et q ut sit $\frac{p}{q} = \frac{a \pm c}{b \pm d}$, vel $\frac{p}{q} = \frac{a \pm d}{b \pm c}$, ac numeri $4n+1$ et $pp+qq$ certo habebunt divisorem communem, qui ergo facile assignatur (*).

3. Proposito itaque hujusmodi numero $4n+1$, operationem ita institui convenit, ut ab eo continuo numeri quadrati subtrahantur, eaque residua tantum notentur, quae etiam sint numeri quadrati; ubi quidem statim apparet, hanc subtractionem non ultra quadrata semissi minora continuari opus esse. Si enim fuerit $4n+1 = aa+bb$, horum quadratorum alterum certe erit minus semisse $\frac{4n+1}{2}$. Vel cum horum binorum quadratorum alterum necessario sit par, alterum impar, sufficiet vel paria tantum, vel imparia quadrata ipso numero proposito minora subtrahi, quo pacto

(*) V. Comment. XII. pag. 155.

multitudo quadratorum subtrahendorum haud mediocriter imminuitur. Cum autem numerus omnium quadratorum ipso numero proposito minorum sit $= \sqrt{(4n+1)}$, eorum autem, quae ejus semisse sunt minora, $= \sqrt{\frac{4n+1}{2}}$, erit quadratorum semisse majorum numerus

$$= \left(1 - \frac{1}{\sqrt{2}}\right)\sqrt{(4n+1)} = \frac{5}{17}\sqrt{(4n+1)} \text{ proxime:}$$

quae quoniam etiam subtrahi sufficit, hoc modo numerus subtractionum ad trientem fere redigitur.

4. Maxime ergo expedire videtur hanc operationem ita institui, ut a quadrato maximo infra numerum propositum $4n+1$ initium capiatur, indeque quadrata continuo minora subtrahantur, donec ad quadrata semissi minora perveniatur. Veluti si numerus propositus sit 101, sufficiet inde haec tria quadrata 100, 81, 64 subtraxisse, quia sequens 49 jam foret semissi $50\frac{1}{2}$ minus; hoc modo cum inter tria residua 1, 20, 37 unicum occurrat quadratum 1, hoc certum est signum, numerum 101 esse primum. Verumtamen si numerus propositus $4n+1$ fuerit praemagnus, etiam hae operationes nimis multiplicantur; ex quo in id potissimum erit incumbendum, ut harum subtractionum numerus imminuatur, quod fiet si eae excludantur, quae ad talia residua perducunt, quae a quadratorum natura abhorreant, cujusmodi sunt residua in his formis contenta: $3m+2$, $5m+2$, $5m+3$, $8m+5$, etc. formae enim $8m+3$ et $8m+7$ ob indolem numeri propositi $4n+1$ numquam occurrunt.

5. Dantur autem certae numerorum formae $4n+1$ species, unde plurima quadrata inde subtrahenda excluduntur. Veluti si sit $4n+1 = 3m+2$, ac ponatur hic numerus $= xx+yy$, uterque numerus x et y in forma $3p \pm 1$ contineatur necesse est, ita ut numeri formae $3p$ excludantur, simili modo si sit $4n+1 = 5m+2$, utrumque numerum x et y in forma $5p \pm 1$ contineri oportet, et si $4n+1 = 5m+3$ in forma $5p \pm 2$. Denique si $8m+5 = xx+yy$, numerorum quidem x et y alter est impar alter par, hic vero adeo impariter par, seu formae $4p+2$. Quodsi ergo simul fuerit

$$xx+yy = 3m+2 = 5m+2$$

numeros x et y simul in his duabus formis $3p \pm 1$ et $5p \pm 1$ contineri oportet, unde eorum forma concluditur:

$$x \text{ vel } y = 15p \pm (1,\ 4).$$

At si fuerit

$$xx+yy = 3m+2 = 5m+3,$$

forma numerorum x et y est et $3p \pm 1$, et $5p \pm 2$, quae duplex forma in hanc unam contrahitur

$$x \text{ vel } y = 15p \pm (2,\ 7).$$

6. Quoniam hoc modo duae tertiae partes omnium numerorum, quos tentari oporteret, excluduntur, hi casus imprimis sunt apti, quibus examen satis expedite instituere licebit. Quare numerorum $N = 4n+1$ eas species potissimum contemplemur, quae vel in his duabus formis $3m+2$ et $5m+2$, vel in his $3m+2$ et $5m+3$ contineantur. Numeri autem prioris speciei ad hanc formam $15m+2$ reducuntur, qui cum insuper in forma $4n+1$ contineri debeant, haec species sequenti formula exprimetur:

Species prima: $N = 60n + 17$,

qui numerus alio modo summa duorum quadratorum esse nequit, nisi utriusque quadrati radix sit numerus formae $15p \pm (1, 4)$, scilicet vel $15p \pm 1$, vel $15p \pm 4$; unde numeri tentandi ex his quatuor progressionibus sunt capiendi:

1, 16, 31, 46, 61, 76, 91, 106, 121, 136 etc.
4, 19, 34, 49, 64, 79, 94, 109, 124, 139 etc.
11, 26, 41, 56, 71, 86, 101, 116, 131, 146 etc.
14, 29, 44, 59, 74, 89, 104, 119, 134, 149 etc.

et reliquos omnes in hoc negotio praetermittere licet.

7. Simili modo alteram speciem evolvamus, quae duplici forma $3m + 2$ et $5m + 3$ continetur, et propterea ad hanc unam $15m + 8$ revocatur. Hinc autem tantum illi numeri sunt usui, qui simul sunt formae $4n + 1$, ex quo haec species sequenti formula exprimetur:

Species secunda $N = 60n + 53$.

Hujus ergo formae si fuerit numerus explorandus, utrum sit primus nec ne? ab eo alia quadrata subtrahi non est opus, nisi quorum radices in hac forma $15p \pm (2, 7)$ contineantur; quas ergo ex sequentibus quaternis progressionibus arithmeticis sumi oportet:

2, 17, 32, 47, 62, 77, 92, 107, 122, 137, 152 etc.
7, 22, 37, 52, 67, 82, 97, 112, 127, 142, 157 etc.
8, 23, 38, 53, 68, 83, 98, 113, 128, 143, 158 etc.
13, 28, 43, 58, 73, 88, 103, 118, 133, 148, 163 etc.

hoc ergo modo multitudo quadratorum subtrahendorum fere ad trientem reducitur.

8. Neque vero his omnibus quadratis tentamen institui opus est, prout enim numerus propositus N insuper fuerit comparatus, inde praeterea multa excluduntur. Cum enim omnes numeri formae $N = 4n + 1$ in has quatuor resolvantur:

$$16n + 1, \quad 16n + 5, \quad 16n + 9, \quad 16n + 13$$

si statuatur $N = xx + yy$, et x denotet numerum parem, y vero imparem, pro his speciebus numeri x et y sequenti modo comparati reperiuntur:

si sit	erit	et
$N = 16n + 1$	$x = 4m$	$y = 8p \pm 1$
$N = 16n + 5$	$x = 4m \pm 2$	$y = 8p \pm 1$
$N = 16n + 9$	$x = 4m$	$y = 8p \pm 3$
$N = 16n + 13$	$x = 4m \pm 2$	$y = 8p \pm 3$.

9. Combinemus has quaternas species cum binis praecedentibus, et obtinebimus sequentes octo species, pro quibus formas tam radicis paris x quam imparis y exhibeamus:

si fuerit N	erit $x =$	et $y =$
$240n + 17$	$60m \pm (4, 16)$	$120p \pm (1, 31, 41, 49)$
$240n + 77$	$60m \pm (14, 26)$	$120p \pm (11, 19, 29, 59)$
$240n + 137$	$60m \pm (4, 16)$	$120p \pm (11, 19, 29, 59)$
$240n + 197$	$60m \pm (14, 26)$	$120p \pm (1, 31, 41, 49)$
$240n + 53$	$60m \pm (2, 22)$	$120p \pm (7, 17, 23, 47)$
$240n + 113$	$60m \pm (8, 28)$	$120p \pm (7, 17, 23, 47)$
$240n + 173$	$60m \pm (2, 22)$	$120p \pm (13, 37, 43, 53)$
$240n + 233$	$60m \pm (8, 28)$	$120p \pm (13, 37, 43, 53)$

10. Dantur autem in his numeris species, quibus adhuc plures numeri tentandi excluduntur, quae ita se habent

si sit	erit	et
$N = 32n + 5$	$x = 4m \pm 2$	$y = 16p \pm 1$
$N = 32n + 13$	$x = 4m \pm 2$	$y = 16p \pm 3$
$N = 32n + 21$	$x = 4m \pm 2$	$y = 16p \pm 7$
$N = 32n + 29$	$x = 4m \pm 2$	$y = 16p \pm 5$

quae cum binis principalibus combinatae praebent

si sit N	erit $x =$	et $y =$
$480n + 77$	$60m \pm (14, 26)$	$240p \pm (19, 29, 61, 109)$
$480n + 197$	$60m \pm (14, 26)$	$240p \pm (1, 31, 49, 79)$
$480n + 317$	$60m \pm (14, 26)$	$240p \pm (11, 59, 91, 101)$
$480n + 437$	$60m \pm (14, 26)$	$240p \pm (41, 71, 89, 119)$
$480n + 53$	$60m \pm (2, 22)$	$240p \pm (7, 23, 73, 103)$
$480n + 173$	$60m \pm (2, 22)$	$240p \pm (13, 67, 77, 83)$
$480n + 293$	$60m \pm (2, 22)$	$240p \pm (17, 47, 97, 113)$
$480n + 413$	$60m \pm (2, 22)$	$240p \pm (37, 43, 53, 107)$

Hic ergo ex valoribus ipsius y, quos praecedentes species admittunt, denuo semissis excluditur.

11. Quoniam hic valores radicis imparis y multo magis imminuuntur, quam radicis paris x, calculus multo evadet facilior et brevior, si a numero proposito N, siquidem in una postremarum specierum contineatur, successive omnia quadrata imparia ipso minora subtrahantur, residuaque examinentur an sint quadrata nec ne? harum operationum numerus satis erit modicus, etiamsi numerus propositus fuerit praemagnus, et quoniam radices per differentiam 240 increscunt, insignia compendia in calculo usurpari poterunt. Scilicet si quaecunque quatuor minimarum radicum dicatur $= a$, quia a numero proposito N, si modo in aliqua octo postremarum specierum contineatur, vel quod eodem redit, si fuerit vel hujus formae $120n + 77$, vel hujus $120n + 53$, successive subtrahi debent quadrata aa, $(240 \pm a)^2$, $(480 \pm a)^2$ etc. notetur differentias esse primas

$$57600 \pm 480a, \quad 3.57600 \pm 480a \text{ etc.}$$

secundas vero esse constantes $= 115200$, quo pacto totum negotium ad meras additiones et subtractiones reducitur; et quia quaelibet radix simplex a tam positive quam negative accipi potest, utraque pari calculo expedietur.

12. **Problema.** Proposito numero quantumvis magno N, qui vel in hac forma $120n + 77$, vel in hac $120n + 53$ contineatur, explorare utrum is sit primus nec ne?

Solutio. Statuatur $N = aa + zz$, et pro octonis formis ipsius N littera a quatuor habebit valores sequentes:

si sit	erunt quaterni valores ipsius a
$N = 480n + 77$	19, 29, 61, 109
$N = 480n + 197$	1, 31, 49, 79
$N = 480n + 317$	11, 59, 91, 101
$N = 480n + 437$	41, 71, 89, 119
$N = 480n + 53$	7, 23, 73, 103
$N = 480n + 173$	13, 67, 77, 83
$N = 480n + 293$	17, 47, 97, 113
$N = 480n + 413$	37, 43, 53, 107.

Pro quolibet ergo numero N habebimus quatuor valores ipsius a, quorum singuli dabunt binas numerorum series descendentes

$$N - aa,\quad N - (240 + a)^2,\quad N - (480 + a)^2,\quad N - (720 + a)^2 \text{ etc.}$$
$$N - aa,\quad N - (240 - a)^2,\quad N - (480 - a)^2,\quad N - (720 - a)^2 \text{ etc.}$$

quarum illius differentia prima est $57600 + 480a$, hujus vero $57600 - 480a$, utriusque vero differentia secunda constans $= 115200$. Ambae hae progressiones continuentur donec ad terminos negativos perveniatur, ex iisque ii notentur, qui sunt numeri quadrati. Quodsi tum eveniat, ut unicus occurrat numerus quadratus, hoc erit signum indubium, propositum numerum N esse primum; sin autem vel nullus numerus quadratus occurrat, vel plures uno, certo hinc erit concludendum, numerum propositum N non esse primum, sed ex factoribus componi.

13. **Coroll. 1.** Quodsi ergo numerus propositus N in altera harum formarum $120n + 77$ et $120n + 53$ contineatur, tum satis expedite examen institui poterit, utrum is numerus sit primus nec ne? cum quadrata, quae successive subtrahi oportet, scilicet $(240\lambda \pm a)^2$, mox ipsum numerum N sint superatura.

14. **Coroll. 2.** Si enim numerus propositus N unum millionem non superet, quadrata subtrahendo infra $(1200 \pm a)^2$ subsistent, eorumque ergo numerus pro quolibet numero a non ad 9 usque ascendet; et quoniam quaterni hujusmodi numeri a habentur, paucioribus quam 36 operationibus totum negotium conficietur.

15. **Coroll. 3.** Si numerus N adeo decuplo fuerit major, operationum numerus ad triplum tantum increscet, et quoniam pro quovis numero a quadrata subtrahenda ejusmodi progressionem constituunt, quarum differentiae secundae sunt constantes, hinc ingentia calculi compendia nascuntur.

16. **Scholion.** Etsi haec methodus ad nonnullas tantum numerorum species patet, quippe quae in altera harum formarum $120n + 77$ et $120n + 53$ sint contentae, ea tamen neutiquam attentione indigna videtur. Cum enim ejusmodi methodum, quae se prorsus ad omnes numeros extendat, ne sperare quidem liceat, quae scilicet a vulgari regula, qua divisionem per omnes numeros primos, radice quadrata numeri propositi minores, tentari oportet, discrepet, eaque sit multo expeditior, omnia compendia, quae quidem in hoc negotio invenire licet, neutiquam sunt contemnenda, etiamsi ea ad paucissimas numerorum species extendantur, dummodo numeros quantumvis magnos in se complectantur. Cum enim problema jam olim propositum, quo numerus primus dato numero major desideratur, adhuc vires ingenii humani superare videatur, non parum praestitisse censendus est, qui numeros valde magnos, qui certo sint primi, in medium afferre valuerit. Usum igitur methodi hic expositae aliquot exemplis declarabo.

17. **Exemplum 1.** *Explorare utrum hic numerus 481037 sit primus nec ne?*

Cum hic numerus sit $= 1002 . 480 + 77$, in prima forma continetur, ubi quatuor valores ipsius a sunt 19, 29, 61, 109, calculus ergo sequenti modo instituatur:

$a = \pm 19$

481037	57600
361	9120
* 480676	480676 *
66720	48480
1152	1152
* 413956	432196 *
181920	163680
1152	1152
* 232036	268516 *

$a = \pm 29$

481037	57600
841	13920
* 480196	480196 *
71520	43680
1152	1152
* 408676	436516 *
186720	158880
* 221956	1152
	277636 *
	274080
	3556 *

$a = \pm 61$

481037	57600
3721	29280
* 477316	477316 *
86880	28320
* 390436	448996 *
202080	143520
□ 188356	305476 *
	258720
	46756 *

$a = \pm 109$

481037	57600
11881	52320
* 469156	469156 *
109920	5280
* 359236	463876 *
225120	120480
* 134116	343396 □
	235680
	107716 *

In his residuis duo occurrunt quadrata signo □ notata, dum reliqua non-quadrata asterisco * notavi, ex quo concludo numerum propositum non esse primum. Cum autem sit duplici modo duorum

quadratorum summa scilicet $481037 = 434^2 + 541^2 = 586^2 + 371^2$, ejus divisores, quos quoque summas esse duorum quadratorum necesse est, assignare licebit, sit enim $pp + qq$ divisor, erit $\frac{p}{q} = \frac{434 \pm 586}{541 \pm 371}$, vel $\frac{p}{q} = \frac{586 \pm 541}{434 \pm 371}$, hinc $\frac{p}{q} = \frac{6}{1}$, vel $\frac{p}{q} = \frac{85}{76}$, ergo divisores sunt 37 et 13001.

18. **Exemplum 2.** *Explorare utrum hic numerus* 829853 *sit primus nec ne?*

Cum hic numerus sit $= 1728.480 + 413$, ad ultimam speciem pertinet, ubi valores ipsius a sunt 37, 43, 53, 107 calculus ergo sequenti modo instituatur.

$a = \pm 37$

829853	57600
1369	17760
* 828484	828484 *
75360	39840
1152	1152
* 753124	788644 *
190560	155040
1152	1152
* 562564	633604 *
305760	270240
* 256804	363364 *

$a = \pm 43$

829853	57600
1849	20640
* 828004	828004 *
78240	36960
1152	1152
* 749764	791044 *
193440	152160
1152	1152
* 556324	638884 *
308640	267360
* 247684	371524 *

$a = \pm 53$

829853	57600
2809	25440
* 827044	827044 *
83040	32160
1152	1152
* 744004	794884 *
198240	147360
1152	1152
* 545764	647524 *
313440	262560
	1152
□ 232324	384964 *
	377760
	7204 *

$a = \pm 107$

829853	57600
11449	51360
* 818404	818404 *
108960	6240
1152	1152
* 709444	812164 *
224160	121440
1152	1152
* 485284	690724 *
339360	236640
	1152
□ 145924	454084 *
	351840
	102244 *

Quoniam hic duo occurrunt quadrata, unde fit

$$829853 = 482^2 + 773^2 = 382^2 + 827^2$$

hic numerus non est primus sed factores habet 257 et 3229.

19. **Exemplum 3.** *Explorare utrum hic numerus 2400317 sit primus nec ne?*

Ex hujus numeri forma $= 5000.480 + 317$ intelligitur, eum ad speciem tertiam pertinere, pro qua valores ipsius a sunt 11, 59, 91, 101, unde calculus ita se habebit:

$a = \pm 11$

	2400317	57600	
	121	5280	
*	2400196	2400196	*
	62880	52320	
	1152	1152	
*	2337316	2347876	*
	178080	167520	
	1152	1152	
*	2159236	2180356	*
	293280	282720	
	1152	1152	
□	1865956	1897636	*
	408480	397920	
	1152	1152	
*	1457476	1499716	*
	523680	513120	
	1152	1152	
*	933796	986596	*
	638880	628320	
*	294916	358276	*

$a = \pm 59$

	2400317	57600	
	3481	28320	
*	2396836	2396836	*
	85920	29280	
	1152	1152	
*	2310916	2367556	*
	201120	144480	
	1152	1152	
*	2109796	2223076	*
	316320	259680	
	1152	1152	
*	1793476	1963396	*
	431520	374880	
	1152	1152	
*	1361956	1588516	*
	546720	490080	
	1152	1152	
*	815236	1098436	*
	661920	605280	
*	153316	493156	*

$a = \pm 91$

	2400317	57600	
	8281	43680	
*	2392036	2392036	*
	101280	13920	
	1152	1152	
*	2290756	2378116	*
	216480	129120	
	1152	1152	
*	2074276	2248996	*
	331680	244320	
	1152	1152	
*	1742596	2004676	*
	446880	359520	
	1152	1152	
*	1295716	1645156	*
	562080	474720	
	1152	1152	
*	733636	1170436	*
	677280	589920	
*	56356	580516	*

$a = \pm 101$

	2400317	57600	
	10201	48480	
□	2390116	2390116	□
	106080	9120	
	1152	1152	
*	2284036	2380996	*
	221280	124320	
	1152	1152	
*	2062756	2256676	*
	336480	239520	
	1152	1152	
*	1726276	2017156	*
	451680	354720	
	1152	1152	
*	1274596	1662436	*
	566880	469920	
	1152	1152	
*	707716	1192516	*
	682080	585120	
*	25636	607396	*

Ex duobus quadratis, quae hic occurrunt, numerus propositus concluditur habere factores 53.45289.

20. **Exemplum 4.** *Explorare utrum hic numerus* 3861317 *sit primus nec ne?*

Cum hic numerus sit $= 8044.480 + 197$, ad secundam speciem pertinet et calculus ita se habebit:

	$a = \pm 1$				$a = \pm 31$		
	3861317	57600			3861317	57600	
	1	480			961	14880	
•	3861316	3861316	•	•	3860356	3860356	•
	58080	57120			72480	42720	
	1152	1152			1152	1152	
•	3803236	3804196	•	•	3787876	3817636	•
	173280	172320			187680	157920	
	1152	1152			1152	1152	
•	3629956	3631876	•	•	3600196	3659716	•
	288480	287520			302880	273120	
	1152	1152			1152	1152	
•	3341476	3344356	•	•	3297316	3386596	•
	403680	402720			418080	388320	
	1152	1152			1152	1152	
□	2937796	2941636	•	•	2879236	2998276	•
	518880	517920			533280	503520	
	1152	1152			1152	1152	
•	2418916	2423716	•	•	2345956	2494756	•
	634080	633120			648480	618720	
	1152	1152			1152	1152	
•	1784836	1790596	•	•	1697476	1876036	•
	749280	748320			763680	733920	
	1152	1152			1152	1152	
•	1035556	1042276	•	•	933796	1142116	•
	864480	863520			878880	849120	
•	171076	178756	•	•	54916	292996	•

$a = \pm 49$		$a = \pm 79$	
3861317	57600	3861317	57600
2401	23520	6241	37920
* 3858916	3858916 *	* 3855076	3855076 *
81120	34080	95520	19680
1152	1152	1152	1152
* 3777796	3824836 *	* 3759556	3835396 *
196320	149280	210720	134880
1152	1152	1152	1152
* 3581476	3675556 *	* 3548836	3700516 *
311520	264480	325920	250080
1152	1152	1152	1152
* 3269956	3411076 *	* 3222916	3450436 *
426720	379680	441120	365280
1152	1152	1152	1152
* 2843236	3031396 *	* 2781796	3085156 *
541920	494880	556320	480480
1152	1152	1152	1152
* 2301316	2536516 *	* 2225476	2604676 *
657120	610080	671520	595680
1152	1152	1152	1152
* 1644196	1926436 *	* 1553956	2008996 *
772320	725280	786720	710880
	1152		1152
* 871876	1201156 *	* 767236	1298116 *
	840480		826080
	360676 *		472036 *

Quoniam igitur in his residuis unicum quadratum reperitur, numerus propositus certe est primus; aequatur autem summae horum duorum quadratorum $1714^2 + 961^2$.

21. **Schollon.** Cum igitur jam certi simus numerum 3861317 esse primum, hic fortasse maximus est numerus primus quem novimus; ac si quis hunc numerum secundum regulam vulgarem explorare voluerit, divisionem per omnes numeros primos usque ad 1965 tentare deberet, qui labor certe non solum maxime foret prolixus, sed etiam summopere taediosus; cum tamen hoc modo totum negotium brevi temporis spatio facillime expediri possit. Simili modo tentavi numerum $3862997 = 8047 \cdot 480 + 437$, ad quartam speciem referendum, quem pariter primum esse deprehendi. Nisi autem numerus propositus in octo memoratis speciebus contineatur, etiamsi sit formae $4n + 1$, examen laborem magis operosum postulat; quamvis negotium ita dirigi queat, ut

non pluribus subtractionibus sit opus. Verum cum universa haec investigatio plerisque omni usu destituta videatur, hoc argumentum fusius non prosequar sed theoremata tantum, quibus haec methodus innititur, breviter subjungo.

Theorema. 1. Si sit $xx+yy=9n+1$, erit
vel $x=3p$, vel $x=9p\pm1$.

Theorema 2. Si sit $xx+yy=9n+4$, erit
vel $x=3p$, vel $x=9p\pm2$.

Theorema 3. Si sit $xx+yy=9n+7$, erit
vel $x=3p$, vel $x=9p\pm4$.

Theorema 4. Si sit $xx+yy=3n+2$, erit $x=3p\pm1$.

Theorema 5. Si sit $xx+yy=5n+2$, erit $x=5p\pm1$.

Theorema 6. Si sit $xx+yy=5n+3$, erit $x=5p\pm2$.

Theorema 7. Si sit $xx+yy=25n+1$, erit
vel $x=5p$, vel $x=25p\pm1$.

Theorema 8. Si sit $xx+yy=25n+4$, erit
vel $x=5p$, vel $x=25p\pm2$.

Theorema 9. Si sit $xx+yy=25n+6$, erit
vel $x=5p$, vel $x=25p\pm9$.

Theorema 10. Si sit $xx+yy=25n+9$, erit
vel $x=5p$, vel $x=25p\pm3$.

Theorema 11. Si sit $xx+yy=25n+11$, erit
vel $x=5p$, vel $x=25p\pm6$.

Theorema 12. Si sit $xx+yy=25n+14$, erit
vel $x=5p$, vel $x=25p\pm8$.

Theorema 13. Si sit $xx+yy=25n+16$, erit
vel $x=5p$, vel $x=25p\pm4$.

Theorema 14. Si sit $xx+yy=25n+19$, erit
vel $x=5p$, vel $x=25p\pm12$.

Theorema 15. Si sit $xx+yy=25n+21$, erit
vel $x=5p$, vel $x=25p\pm11$.

Theorema 16. Si sit $xx+yy=25n+24$, erit
vel $x=5p$, vel $x=25p\pm7$.

Conclusio. Ex his theorematibus sequitur: si summa duorum quadratorum habuerit hanc formam $xx + yy = 14400n + 11401$, tum quadrati imparis xx radicem fore

$$\begin{aligned} &\text{vel I.} \quad x = 480m \pm (75,\ 195), \\ &\text{vel II.} \quad x = 1440m \pm (85,\ 355,\ 445,\ 715), \\ &\text{vel III.} \quad x = 2400m \pm (99,\ 501,\ 651,\ 1149), \\ &\text{vel IV.} \quad x = 7200m \pm \begin{Bmatrix} 149, & 949, & 1301, & 1949 \\ 2101, & 2749, & 3101, & 3299 \end{Bmatrix}. \end{aligned}$$

Ex hoc numerorum ordine sumto $n = 700$, exploravi hunc numerum 10091401, cujus resolutionem in duo quadrata unico modo succedere deprehendi, scilicet $1251^2 + 2920^2$, quod certum est indicium hunc numerum esse primum. Habemus ergo numerum decem millionibus majorem, 10091401, quem certo novimus esse primum; si quis autem alia quacunque methodo uti voluerit, nunquam profecto tantum numerum primum exhibebit.

XXVII.

De partitione numerorum in partes tam numero quam specie datas.

(N. Comment. XIV. I. 1769. p. 168. Exhib. 1768 Aug. 18.)

1. Cum olim tractavissem problema de partitione numerorum (*), quo quaerebatur, quot variis modis datus numerus in duas, vel tres, vel quatuor, vel generatim in tot partes, quot quis voluerit, discerpi possit, id potissimum curavi, ut in ejus solutione nihil quicquam inductioni, cujus usus plerumque in hujusmodi problematibus solvendis solet esse frequentissimus, tribuerem. Atque methodus, qua sum usus, ita videtur comparata, ut etiam ad alia problemata aequo successu adhiberi possit, id quod vulgatissimo illo problemate, quo quaeri solet, quot modis datus numerus dato tesserarum numero projici possit, eo quidem amplissime extenso hic ostendere constitui.

2. Quando autem quaeritur, quot modis datus numerus N datum tesserarum numerum n projiciendo cadere possit, quaestio huc redit, quot variis modis datus numerus N in n partes resolvi possit, quarum singulae sint vel 1, vel 2, vel 3, vel 4, vel 5, vel 6, siquidem facies tesserarum his numeris sint insignitae. Ex quo nascitur haec quaestio latius patens: quot variis modis datus numerus N dividi possit in n partes, quarum singulae sint vel α, vel β, vel γ, vel δ etc., quorum numerorum α, β, γ, δ, etc. multitudo sit pariter data, puta $= m$, ita ut partes, in quas datus numerus sit resolvendus tam numero quam specie dentur.

3. Concipiantur scilicet ejusmodi tesserae, quae non ut vulgo sex, sed m habeant facies seu hedras, ita ut in singulis hae facies notatae sint numeris α, β, γ, δ, etc. atque jam quaeritur, si habeantur n hujusmodi tesserae, quot modis iis projiciendis datus numerus N produci possit. Possent etiam tesserae inter se dispares assumi, ita ut singulae peculiarem haberent hedrarum numerum, quae etiam in singulis peculiaribus numeris sint inscriptae; verum ex iis, quae de tesseris vulgaribus sum allaturus, etiam solutio hujus quaestionis latissime patentis haud difficulter colligetur.

4. Numeros autem, quibus facies tesserarum sunt notatae, tanquam exponentes quantitatis cujusdam x considero, ita ut pro tessera vulgari hanc habeamus expressionem

$$x^1 + x^2 + x^3 + x^4 + x^5 + x^6$$

ubi cuique potestati unitatem pro coefficiente tribuo, quandoquidem quilibet numerus exponente designatus aeque facile cadere potest. Quodsi jam hujus expressionis quadratum sumatur, quaevis potestas ipsius x tantum recipiet coefficientem, qui indicet quot modis ea potestas ex multiplicatione binorum terminorum istius expressionis resultare, hoc est, quot modis ejus exponens ex additione binorum numerorum ex ordine 1, 2, 3, 4, 5, 6 produci possit. Evoluto ergo nostrae expressionis quadrato, si in eo occurrat terminus Mx^N, inde colligitur numerum N binis tesseris jaciendis tot modis prodire, quot coefficiens M contineat unitates.

(*) Vide Comment. IX pag. 73 — 101 hujus operis

5. Simili modo evidens est, si istius expressionis sumatur cubus $(x + x^2 + x^3 + x^4 + x^5 + x^6)^3$, in ejus evolutione quamvis potestatem x^N toties occurrere, quot modis ejus exponens N oriri potest addendis tribus numeris ex ordine 1, 2, 3, 4, 5, 6; unde si hujus potestatis coefficiens sit M, totusque sit terminus Mx^N, ex eo concludimus numerum N tribus tesseris jaciendis tot modis produci posse, quot coefficiens M contineat unitates. Generatim ergo si sumatur exponentis n dignitas nostrae expressionis $(x + x^2 + x^3 + x^4 + x^5 + x^6)^n$, ea evoluta secundum potestates ipsius x, quilibet terminus Mx^N docebit, si numerus tesserarum fuerit $= n$, iis jaciendis numerum N tot modis cadere posse, quot coefficiens M contineat unitates.

6. Si ergo tesserarum numerus fuerit $= n$, quaeraturque quot modis datus numerus N iis projiciendis cadere possit, quaestio resolvetur per evolutionem hujus formulae

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^n,$$

cujus cum primus terminus futurus sit x^n, ultimus vero x^{6n}, prodibit hujusmodi terminorum progressio:

$$x^n + Ax^{n+1} + Bx^{n+2} + Cx^{n+3} \ldots\ldots + Mx^N \ldots\ldots + x^{6n},$$

cujus quilibet terminus Mx^N ostendet numerum N exponenti aequalem tot modis cadere posse, quot coefficiens M contineat unitates: ex quo statim elucet, quaestionem locum habere non posse, nisi numerus propositus N contineatur intra limites n et $6n$. Totum ergo negotium huc redit, ut ista progressio seu singulorum terminorum coefficientes assignentur.

7. Ad hos igitur inveniendos ponatur formula evolvenda hoc modo repraesentata

$$x^n(1 + x + x^2 + x^3 + x^4 + x^5)^n = V$$

tum vero pro ejusdem evolutione statuatur

$$V = x^n(1 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 + Fx^6 + \text{etc.})$$

Ac posito $\frac{V}{x^n} = Z$, erit ex priori differentiale logarithmicum:

$$\frac{xdZ}{Zdx} = \frac{nx + 2nx^2 + 3nx^3 + 4nx^4 + 5nx^5}{1 + x + x^2 + x^3 + x^4 + x^5}.$$

Ejusdem autem valor ex posteriori prodit

$$\frac{xdZ}{Zdx} = \frac{Ax + 2Bx^2 + 3Cx^3 + 4Dx^4 + 5Ex^5 + 6Fx^6 \text{ etc.}}{1 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 + Fx^6 \text{ etc.}},$$

quae duae expressiones inter se debent esse aequales, unde coefficientium valores determinabuntur.

8. Constitututa autem harum duarum expressionum aequalitate oritur ista aequatio

$$nx + \left.\begin{matrix} nA \\ +2n \end{matrix}\right\} x^2 + \left.\begin{matrix} nB \\ +2nA \\ +3n \end{matrix}\right\} x^3 + \left.\begin{matrix} nC \\ +2nB \\ +3nA \\ +4n \end{matrix}\right\} x^4 + \left.\begin{matrix} nD \\ +2nC \\ +3nB \\ +4nA \\ +5n \end{matrix}\right\} x^5 + \left.\begin{matrix} nE \\ +2nD \\ +3nC \\ +4nB \\ +5nA \end{matrix}\right\} x^6 + \left.\begin{matrix} nF \\ +2nE \\ +3nD \\ +4nC \\ +5nB \end{matrix}\right\} x^7 + \left.\begin{matrix} nG \\ +2nF \\ +3nE \\ +4nD \\ +5nC \end{matrix}\right\} x^8 \text{ etc.}$$

$$= Ax + \left.\begin{matrix} 2B \\ +A \end{matrix}\right\} x^2 + \left.\begin{matrix} 3C \\ +2B \\ +A \end{matrix}\right\} x^3 + \left.\begin{matrix} 4D \\ +3C \\ +2B \\ +A \end{matrix}\right\} x^4 + \left.\begin{matrix} 5E \\ +4D \\ +3C \\ +2B \\ +A \end{matrix}\right\} x^5 + \left.\begin{matrix} 6F \\ +5E \\ +4D \\ +3C \\ +2B \\ +A \end{matrix}\right\} x^6 + \left.\begin{matrix} 7G \\ +6F \\ +5E \\ +4D \\ +3C \\ +2B \end{matrix}\right\} x^7 + \left.\begin{matrix} 8H \\ +7G \\ +6F \\ +5E \\ +4D \\ +3C \end{matrix}\right\} x^8 \text{ etc.}$$

quae binae expressiones, cum secundum singulos terminos inter se debeant esse aequales, valores singulorum coefficientium suppeditabunt.

9. Hinc autem sequentes determinationes impetrantur:

$$\begin{aligned}
A &= n \\
2B &= (n-1)A + 2n \\
3C &= (n-2)B + (2n-1)A + 3n \\
4D &= (n-3)C + (2n-2)B + (3n-1)A + 4n \\
5E &= (n-4)D + (2n-3)C + (3n-2)B + (4n-1)A + 5n \\
6F &= (n-5)E + (2n-4)D + (3n-3)C + (4n-2)B + (5n-1)A \\
7G &= (n-6)F + (2n-5)E + (3n-4)D + (4n-3)C + (5n-2)B \\
8H &= (n-7)G + (2n-6)F + (3n-5)E + (4n-4)D + (5n-3)C
\end{aligned}$$

etc.

Quilibet ergo coefficiens determinatur per quinos praecedentium, quibus inventis erit

$$V = x^n + Ax^{n+1} + Bx^{n+2} + Cx^{n+3} + Dx^{n+4} + Ex^{n+5} + \text{etc.}$$

sicque problema de n tesseris in genere est solutum.

10. Si a qualibet superiorum aequationum praecedens subtrahatur, obtinebuntur sequentes determinationes multo simpliciores:

$$\begin{aligned}
A &= n \\
2B &= nA + n \\
3C &= nB + nA + n \\
4D &= nC + nB + nA + n \\
5E &= nD + nC + nB + nA + n \\
6F &= nE + nD + nC + nB + nA - 5n \\
7G &= nF + nE + nD + nC + nB - (5n-1)A \\
8H &= nG + nF + nE + nD + nC - (5n-2)B
\end{aligned}$$

etc.

Si denuo differentiae caperentur, relationes istae adhuc simpliciores essent prodituræ, hoc modo

$$\begin{aligned}
2B &= (n+1)A, & 7G &= (n+6)F - (6n-1)A + 5n, \\
3C &= (n+2)B, & 8H &= (n+7)G - (6n-2)B + (5n-1)A, \\
4D &= (n+3)C, & 9J &= (n+8)H - (6n-3)C + (5n-2)B, \\
5E &= (n+4)D, & 10K &= (n+9)J - (6n-4)D + (5n-3)C, \\
6F &= (n+5)E - 6n, & & \text{etc.}
\end{aligned}$$

11. Hinc prout tesserarum numerus fuerit vel 2, vel 3, vel 4, lex progressionis coefficientium erit ut sequitur:

	pro duabus	pro tribus	pro quatuor
$A =$	2	3	4
$2B =$	$3A$	$4A$	$5A$
$3C =$	$4B$	$5B$	$6B$
$4D =$	$5C$	$6C$	$7C$
$5E =$	$6D$	$7D$	$8D$
$6F =$	$7E - 12$	$8E - 18$	$9E - 24$
$7G =$	$8F - 11A + 10$	$9F - 17A + 15$	$10F - 23A + 20$
$8H =$	$9G - 10B + 9A$	$10G - 16B + 14A$	$11G - 22B + 19A$
$9J =$	$10H - 9C + 8B$	$11H - 15C + 13B$	$12H - 21C + 18B$
$10K =$	$11J - 8D + 7C$	$12J - 14D + 12C$	$13J - 20D + 17C$
$11L =$	$12K - 7E + 6D$	$13K - 13E + 11D$	$14K - 19E + 16D$
$12M =$	$13L - 6F + 5E$	$14L - 12F + 10E$	$15L - 18F + 15E$

etc.

quilibet ergo coefficiens per tres praecedentes determinatur, ubi hoc imprimis est notatu dignum, quod tandem in nihilum abeant, et postremi primis evadant pares, id quod ex hac lege minus perspicere licet.

12. Quo autem hanc legem clarius intelligamus denotet haec formula $(N)^{(n)}$ numerum casuum, quibus numerus N per n tesseras produci potest, ita ut sit

$$(n)^{(n)} = 1,\ (n+1)^{(n)} = A,\ (n+2)^{(n)} = B,\ (n+3)^{(n)} = C,\ (n+4)^{(n)} = D, \ldots (n+9)^{(n)} = J$$
$$\text{et}\quad (n+10)^{(n)} = K.$$

Hinc ergo fiet

$$10\,(n+10)^{(n)} = (n+9)\,(n+9)^{(n)} - (6n-4)\,(n+4)^{(n)} + (5n-3)\,(n-3)^{(n)}$$

unde concluditur fore in genere:

$$\lambda(n+\lambda)^{(n)} = (n+\lambda-1)(n+\lambda-1)^{(n)} - (6n+6-\lambda)(n+\lambda-6)^{(n)} + (5n+7-\lambda)(n+\lambda-7)^{(n)}.$$

Ponamus jam $n + \lambda = N$, ut sit $\lambda = N - n$, eritque

$$(N)^{(n)} = \frac{(N-1)(N-1)^{(n)} - (7n+6-N)(N-6)^{(n)} + (6n+7-N)(N-7)^{(n)}}{N-n}$$

ubi notandum est semper fore $(P)^{(n)} = 0$, si fuerit $P < n$.

13. Facilius autem hi coefficientes definiri possunt pro quovis tesserarum numero, si iidem pro tesserarum numero unitate minore jam fuerint reperti. Si enim sit

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^n = x^n + Ax^{n+1} + Bx^{n+2} + Cx^{n+3} + Dx^{n+4} + \text{etc.}$$

ponaturque

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^{n+1} = x^{n+1} + A'x^{n+2} + B'x^{n+3} + C'x^{n+4} + D'x^{n+5} + \text{etc.}$$

erit, quia haec expressio illi per $x + x^2 + x^3 + x^4 + x^5 + x^6$ multiplicatae est aequalis

	hinc differentiis sumendis
$A' = A + 1$	
$B' = B + A + 1$	$B' = A' + B$
$C' = C + B + A + 1$	$C' = B' + C$
$D' = D + C + B + A + 1$	$D' = C' + D$
$E' = E + D + C + B + A + 1$	$E' = D' + E$
$F' = F + E + D + C + B + A$	$F' = E' + F - 1$
$G' = G + F + E + D + C + B$	$G' = F' + G - A$
etc.	etc.

14. Quare si modo denotandi ante introducto utamur, ex aequatione $G' = F' + G - A$ nascitur haec:

$$(n+8)^{(n+1)} = (n+7)^{(n+1)} + (n+7)^{(n)} - (n+1)^{(n)}$$

quae in genere ita repraesentabitur:

$$(n+1+\lambda)^{(n+1)} = (n+\lambda)^{(n+1)} + (n+\lambda)^{(n)} - (n+\lambda-6)^{(n)}.$$

Quod si jam pro $n + \lambda$ scribatur N, erit

$$(N+1)^{(n+1)} = (N)^{(n+1)} + (N)^{(n)} - (N-6)^{(n)},$$

ubi notandum est, quamdiu fuerit $N - 6 < n$, fore $(N-6)^{(n)} = 0$. Hinc simul patet omnes hos numeros fore integros, quod ex priori lege minus apparet.

Tabula

ostendens, quot modis quilibet numerus N per n tesseras cadere possit.

N	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$
1	1	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0
3	1	2	1	0	0	0	0	0
4	1	3	3	1	0	0	0	0
5	1	4	6	4	1	0	0	0
6	1	5	10	10	5	1	0	0
7	0	6	15	20	15	6	1	0
8	0	5	21	35	35	21	7	1
9	0	4	25	56	70	56	28	8
10	0	3	27	80	126	126	84	36
11	0	2	27	104	205	252	210	120
12	0	1	25	125	305	456	462	330
13	0	0	21	140	420	756	917	792
14	0	0	15	146	540	1161	1667	1708
15	0	0	10	140	651	1666	2807	3368
16	0	0	6	125	735	2247	4417	6147
17	0	0	3	104	780	2856	6538	10480
18	0	0	1	80	780	3431	9142	16808
19	0	0	0	56	735	3906	12117	25488
20	0	0	0	35	651	4221	15267	36688

N	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$	$n=8$
21	0	0	0	20	540	4332	18327	50288
22	0	0	0	10	420	4221	20993	65808
23	0	0	0	4	305	3906	22967	82384
24	0	0	0	1	205	3431	24017	98813
25	0	0	0	0	126	2856	24017	113688
26	0	0	0	0	70	2247	22967	125588
27	0	0	0	0	35	1666	20993	133288
28	0	0	0	0	15	1161	18327	135954
29	0	0	0	0	5	756	15267	133288
30	0	0	0	0	1	456	12117	125588
31	0	0	0	0	0	252	9142	113688
32	0	0	0	0	0	126	6538	98813
33	0	0	0	0	0	56	4417	82384
34	0	0	0	0	0	21	2807	65808
35	0	0	0	0	0	6	1667	50288
36	0	0	0	0	0	1	917	36688

15. In his ergo seriebus etiam proprietas § 12 inventa locum habet; ita si fuerit $n=6$, erit:

$$(N)^{(6)}=\frac{(N-1)(N-1)^{(6)}-(48-N)(N-6)^{(6)}+(43-N)(N-7)^{(6)}}{N-6}$$

unde si exempli gratia $N=25$, erit

$$(25)^{(6)}=\frac{24.(24)^{(6)}-23.(19)^{(6)}+18.(18)^{(6)}}{19}$$

at est $(24)^{(6)}=3431$, $(19)^{(6)}=3906$, $(18)^{(6)}=3431$, ideoque

$$(25)^{(6)}=\frac{24.3431-23.3906+18.3431}{19}=\frac{54264}{19}=2856$$

uti tabula habet. Similiter si sit $N=29$, erit

$$(29)^{(6)}=\frac{28.(28)^{(6)}-19.(23)^{(6)}+14.(22)^{(6)}}{23}$$

hinc ob $(28)^{(6)}=1161$, $(23)^{(6)}=3906$ et $(22)^{(6)}=4221$, erit

$$(29)^{(6)}=\frac{32508-74214+59094}{23}=\frac{17388}{23}=756.$$

16. Verum evolutio formulae V (§ 7) alio modo institui potest, ut quilibet terminus absolute assignetur, neque ad hoc praecedentibus sit opus. Cum enim sit

$$1+x+x^2+x^3+x^4+x^5=\frac{1-x^6}{1-x},$$

erit $V=\frac{x^n(1-x^6)^n}{(1-x)^n}$; atque evolutione facta ob

$$(1-x^6)^n=1-\frac{n}{1}x^6+\frac{n(n-1)}{1.2}x^{12}-\frac{n(n-1)(n-2)}{1.2.3}x^{18}+\frac{n(n-1)(n-2)(n-3)}{1.2.3.4}x^{24}-\text{etc.}$$

$$\frac{x^n}{(1-x)^n}=x^n+\frac{n}{1}x^{n+1}+\frac{n(n+1)}{1.2}x^{n+2}+\frac{n(n+1)(n+2)}{1.2.3}x^{n+3}+\frac{n(n+1)(n+2)(n+3)}{1.2.3.4}x^{n+4}+\text{etc.}$$

unde colligitur fore:

$$(n)^{(n)} = 1$$
$$(n+1)^{(n)} = \frac{n}{1}$$
$$(n+2)^{(n)} = \frac{n(n+1)}{1.2}$$
$$(n+3)^{(n)} = \frac{n(n+1)(n+2)}{1.2.3}$$
$$(n+4)^{(n)} = \frac{n\ldots(n+3)}{1\ldots4}$$
$$(n+5)^{(n)} = \frac{n\ldots(n+4)}{1\ldots5}$$
$$(n+6)^{(n)} = \frac{n\ldots(n+5)}{1\ldots6} - \frac{n}{1}\cdot 1$$
$$(n+7)^{(n)} = \frac{n\ldots(n+6)}{1\ldots7} - \frac{n}{1}\cdot\frac{n}{1}$$
$$(n+8)^{(n)} = \frac{n\ldots(n+7)}{1\ldots8} - \frac{n}{1}\cdot\frac{n(n+1)}{1.2}$$
$$(n+9)^{(n)} = \frac{n\ldots(n+8)}{1\ldots9} - \frac{n}{1}\cdot\frac{n(n+1)(n+2)}{1.2.3}$$
$$(n+10)^{(n)} = \frac{n\ldots(n+9)}{1\ldots10} - \frac{n}{1}\cdot\frac{n(n+1)(n+2)(n+3)}{1.2.3.4}$$
$$(n+11)^{(n)} = \frac{n\ldots(n+10)}{1\ldots11} - \frac{n}{1}\cdot\frac{n(n+1)(n+2)(n+3)(n+4)}{1.2.3.4.5}$$
$$(n+12)^{(n)} = \frac{n\ldots(n+11)}{1\ldots12} - \frac{n}{1}\cdot\frac{n(n+1)(n+2)(n+3)(n+4)(n+5)}{1\ldots6} + \frac{n(n-1)}{1.2}\cdot 1$$
$$(n+13)^{(n)} = \frac{n\ldots(n+12)}{1\ldots13} - \frac{n}{1}\cdot\frac{n(n+1)(n+2)(n+3)(n+4)(n+5)(n+6)}{1\ldots7} + \frac{n(n-1)}{1.2}\cdot\frac{n}{1}$$

etc.

unde in genere concluditur:

$$(n+\lambda)^{(n)} = \frac{n\ldots(n+\lambda-1)}{1\ldots\lambda} - \frac{n}{1}\cdot\frac{n\ldots(n+\lambda-7)}{1\ldots(\lambda-6)} + \frac{n(n-1)}{1.2}\cdot\frac{n\ldots(n+\lambda-13)}{1\ldots(\lambda-12)} - \frac{n(n-1)(n-2)}{1.2.3}\cdot\frac{n\ldots(n+\lambda-19)}{1\ldots(\lambda-18)}$$
$$+ \frac{n(n-1)(n-2)(n-3)}{1.2.3.4}\cdot\frac{n\ldots(n+\lambda-25)}{1\ldots(\lambda-24)} - \text{etc.}$$

17. Hinc solutio ad tesseras quocunque alio facierum numero praeditas accommodari potest. Sit enim m numerus facierum in singulis tesseris, quae notatae sint numeris $1, 2, 3\ldots m$, talium autem tesserarum numerus sit $= n$, quibus projectis quaeritur, quot modis datus numerus N cadere possit. Seu quod eodem redit, quaeritur quot modis numerus N in n partes resolvi possit, quae singulae in hoc ordine numerorum $1, 2\ldots m$ sint contentae; ubi quidem notandum est non solum diversas partitiones, sed etiam diversos ordines earundem partium numerari, uti in tesseris fieri solet, ubi exempli gratia jactus 3, 4 et 4, 3 pro duobus diversis casibus habentur.

18. Quodsi ergo haec scriptio $(N)^{(n)}$ denotet casuum numerum, quibus numerus N projiciendis n tesseris, quarum singulae habeant m facies numeris $1, 2, 3\ldots m$ notatas, produci possit; primo notandum est fore $(n)^{(n)} = 1$, et si $N < n$ esse $(N)^{(n)} = 0$. Deinde si $N = mn$, est quoque $(mn)^{(n)} = 1$, et si $N > mn$, erit $(N)^{(n)} = 0$. Denique sive sit $N = n + \lambda$, sive $N = mn - \lambda$, numerus casuum est idem seu $(n+\lambda)^{(n)} = (mn-\lambda)^{(n)}$. Postrema autem formula praebet:

$$(n+\lambda)^{(n)} = \frac{n\ldots(n+\lambda-1)}{1\ldots\lambda} - \frac{n}{1}\cdot\frac{n\ldots(n+\lambda-m-1)}{1\ldots(\lambda-m)} + \frac{n(n-1)}{1.2}\cdot\frac{n\ldots(n+\lambda-2m-1)}{1\ldots(\lambda-2m)}$$
$$-\frac{n(n-1)(n-2)}{1.2.3}\cdot\frac{n\ldots(n+\lambda-3m-1)}{1\ldots(\lambda-3m)} + \text{etc.}$$

19. Facillime autem hi numeri cum ex praecedentibus tum ex casibus, ubi tesserarum numerus est unitate minor, determinabuntur. Erit enim generaliter, si singularum tesserarum numerus facierum fuerit $=m$, eaeque numeris $1, 2\ldots m$ sint insignitae:

$$(N+1)^{(n+1)} = (N)^{(n+1)} + (N)^{(n)} - (N-m)^{(n)},$$
seu
$$(N+1)^{(n)} = (N)^{(n)} + (N)^{(n-1)} - (N-m)^{(n-1)}.$$

Hinc si pro $N+1$ scribatur $n+\lambda$ habebitur

$$(n+\lambda)^{(n)} = (n+\lambda-1)^{(n)} + (n+\lambda-1)^{(n-1)} - (n+\lambda-m-1)^{(n-1)}.$$

Denique pro eodem tesserarum numero n isti numeri ita a praecedentibus pendent, ut sit

$$\lambda(n+\lambda)^{(n)} = (n+\lambda-1)(n+\lambda-1)^{(n)} - (mn+m-\lambda)(n+\lambda-m)^{(n)}$$
$$+(mn-n+m+1-\lambda)(n+\lambda-m-1)^{(n)}.$$

Ceterum notum est summam omnium horum numerorum esse $=m^n$.

20. Simili modo haec quaestio resolvi potest, si non omnes tesserae pari hedrarum numero fuerint praeditae. Ponamus tres dari tesseras, primam hexaëdram numeros 1, 2, 3, 4, 5, 6, secundam octaëdram numeros $1, 2, 3\ldots 8$, et tertiam dodecaëdram numeros $1, 2, 3\ldots 12$ gerentem; quod si jam quaeratur, quot modis datus numerus N cadere possit, evolvatur hoc productum

$$(x+x^2+x^3\ldots x^6)(x+x^2+x^3\ldots x^8)(x+x^2+x^3\ldots x^{12}) = V$$

et coefficiens potestatis x^N ostendet casuum numerum. Cum jam sit

$$V = \frac{x^3(1-x^6)(1-x^8)(1-x^{12})}{(1-x)^3}$$

erit numeratorem evolvendo

$$V = \frac{x^3-x^9-x^{11}-x^{15}+x^{17}+x^{21}+x^{23}-x^{29}}{(1-x)^3}.$$

21. Hic numerator multiplicetur per $\frac{1}{(1-x)^3}$, seu hanc seriem

$$1+3x+6x^2+10x^3+15x^4+21x^5+28x^6+36x^7+\text{etc.}$$

cujus coefficientes sunt numeri trigonales; unde cum numeri n trigonalis $=\frac{n(n+1)}{2}$, quivis hujus seriei terminus erit

$$\frac{n(n+1)}{2}x^{n-1}, \quad \text{seu} \quad \frac{(n-1)(n-2)}{2}x^{n-3}.$$

Jam per numeratorem multiplicando, potestatis x^n coefficiens reperitur:

$$\frac{(n-1)(n-2)}{2} - \frac{(n-7)(n-8)}{2} - \frac{(n-9)(n-10)}{2} - \frac{(n-13)(n-14)}{2} + \frac{(n-15)(n-16)}{2} + \frac{(n-19)(n-20)}{2}$$
$$+\frac{(n-21)(n-22)}{2} - \frac{(n-27)(n-28)}{2},$$

quae expressio autem quovis casu non ulterius continuari debet, quam donec ad factores negativos perveniatur.

22. Relicto autem denominatore $(1-x)^3 = 1 - 3x + 3x^2 - x^3$, series quaesita erit recurrens ex scala relationis $3, -3, +1$ nata, dummodo terminorum numeratoris ratio habeatur. Hinc pro quovis exponente sequentes coefficientes inveniuntur

Exp.	Coeff.	Exp.	Coeff.
3	1	15	47
4	3	16	45
5	6	17	42
6	10	18	38
7	15	19	33
8	21	20	27
9	27	21	21
10	33	22	15
11	38	23	10
12	42	24	6
13	45	25	3
14	47	26	1

Numeri hic majores quam 26 produci nequeunt, cum sit $26 = 6 + 8 + 12$, et omnium casuum summa est $576 = 6.8.12$.

23. Cum hoc modo resolutio numerorum in partes numero et specie datas sine inductionis subsidio absolvi possit, in mentem mihi incidunt quaedam Fermatii elegantia theoremata, quae cum nondum sint demonstrata, fortasse haec methodus ad demonstrationes eorum perductura videtur. Cum enim Fermatius asseverasset omnes numeros vel esse trigonales, vel duorum, vel trium trigonalium aggregata, quia cyphra etiam in ordine trigonalium reperitur, theorema ita enunciari potest, ut omnes numeri in tres trigonales resolubiles dicantur. Quare si numeris trigonalibus pro exponentibus sumtis formetur haec series:

$$1 + x^1 + x^3 + x^6 + x^{10} + x^{15} + x^{21} + x^{28} + \text{etc.} = S$$

demonstrari oportet, si hujus seriei cubus evolvatur, tum omnes plane potestates ipsius x esse occursuras, nullamque omissum iri; quod si demonstrari posset, haberetur demonstratio istius theorematis Fermatiani.

24. Simili modo si hujus seriei

$$1 + x^1 + x^4 + x^9 + x^{16} + x^{25} + x^{36} + \text{etc.} = S$$

sumatur potestas quarta, ostendique queat, in ea omnes plane potestates ipsius x reperiri, habebitur demonstratio hujus theorematis Fermatiani, quo omnes numeri ex additione quaternorum quadratorum resultare statuuntur. In genere autem si ponatur

$$S = 1 + x^1 + x^m + x^{3m-3} + x^{6m-8} + x^{10m-15} + x^{15m-24} + x^{21m-35} + \text{etc.}$$

hujusque seriei sumatur potestas exponentis m, demonstrandum est in ea omnes potestates ipsius x esse prodituras, ita ut omnis numerus sit aggregatum m numerorum polygonalium laterum numero existente $= m$, vel pauciorum.

25. Ex iisdem principiis alia se offert via ad has demonstrationes investigandas, quae a praecedente hoc differt, quod uti ibi non solum diversitas partium, sed etiam ordo spectatur, hic ordinis ratio omittitur. Pro resolutione scilicet in triangulares numeros constituatur haec formula

$$\frac{1}{(1-z)(1-xz)(1-x^3z)(1-x^6z)(1-x^{10}z)(1-x^{15}z)\text{ etc.}},$$

quae evoluta hanc praebeat seriem:

$$1+Pz+Qz^2+Rz^3+Sz^4+Tz^5+\text{etc.}$$

ita ut P, Q, R, S, etc. sint functiones ipsius x tantum. Manifestum autem est fore:

$$P=1+x+x^3+x^6+x^{10}+x^{15}+x^{21}+\text{etc.}$$

at Q praeterea eas potestates ipsius x continebit, quarum exponentes sunt aggregata duorum trigonalium. Demonstrari ergo debet, in functione R omnes plane potestates ipsius x esse occursuras.

26. Simili modo pro resolutione numerorum in quaterna quadrata evolvatur haec fractio

$$\frac{1}{(1-z)(1-xz)(1-x^4z)(1-x^9z)(1-x^{16}z)(1-x^{25}z)\text{ etc.}},$$

quae si abeat in hanc formam:

$$1+Pz+Qz^2+Rz^3+Sz^4+\text{etc.}$$

demonstrandum est functionem S omnes potestates ipsius x complecti. Nam P aequatur seriei $1+x+x^4+x^9+x^{16}+\text{etc.}$ et Q praeterea eas continet potestates ipsius x, quarum exponentes sunt aggregata duorum quadratorum, in qua ergo serie multae adhuc potestates desunt. In R autem insuper eae potestates, quarum exponentes sunt aggregata ternorum quadratorum, aderunt; atque in S quoque eae, quarum exponentes sunt summae quaternorum quadratorum, ita ut in S omnes numeri in exponentibus occurrere debeant.

27. Ex hoc principio definiri potest, quot solutiones problemata, quae ab arithmeticis ad regulam Virginum referri solent, admittant. Hujusmodi problemata huc redeunt, ut inveniri debeant numeri p, q, r, s, t etc. ita ut his duabus conditionibus satisfiat:

$$ap+bq+cr+ds\text{ etc.}=n\quad\text{et}\quad\alpha p+\beta q+\gamma r+\delta s\text{ etc.}=\nu$$

et jam quaestio est, quot solutiones in numeris integris positivis locum sint habiturae: ubi quidem tenendum est numeros a, b, c, d etc. n et α, β, γ, δ etc. ν esse integros, quia nisi tales essent, facile eo reducerentur. Statim quidem apparet, si duo tantum numeri inveniendi p et q proponantur, plus una solutione non dari, quae adeo, nisi pro p et q numeri integri positivi prodeant, pro nulla haberi solet.

28. Jam ad numerum omnium solutionum quovis casu definiendum, ne inductioni seu tentationi quicquam tribuatur, consideretur haec expressio

$$\frac{1}{(1-x^ay^\alpha)(1-x^by^\beta)(1-x^cy^\gamma)(1-x^dy^\delta)\text{ etc.}}$$

eaque evolvatur, unde prodibit hujusmodi series $1+Ax^{\cdot\cdot}y^{\cdot\cdot}+Bx^{\cdot\cdot}y^{\cdot\cdot}+Cx^{\cdot\cdot}y^{\cdot\cdot}$ etc. in qua si occurrat terminus Nx^ny^ν, coefficiens N numerum solutionum indicabit: ac si eveniat, ut hic terminus non occurrat, id indicio erit nullam dari solutionem. Totum ergo negotium in hoc versatur, ut coefficiens hujus termini x^ny^ν investigetur.

XXVIII.

De inventione quotcunque mediarum proportionalium citra radicum extractionem.

(N. Comment. XIV. I. 1769 p. 188. Exhib. 1768. Aug. 18.)

1. **Propositio I.** Si numeri a, b, c, d etc. sint continue proportionales, etiam differentiae $b-a$, $c-b$, $d-c$ etc. erunt in proportione geometrica continua ejusdem exponentis; ac si prior series a proportione geometrica aberret, posterior multo magis aberrabit.

Demonstratio. Prior propositionis pars in elementis est demonstrata: pro altera autem parte ponamus exponentem rationis geometricae $=r$, ut secundum proportionem geometricam foret $b=ar$, $c=ar^2$, $d=ar^3$ etc. Sit autem $b=ar+z$ manente $c=arr$, ita ut z sit error termini b a proportione geometrica, eruntque differentiae $b-a=a(r-1)+z$ et $c-b=ar(r-1)-z$, quarum ratio est $\frac{ar(r-1)-z}{a(r-1)+z}=r-\frac{(r+1)z}{a(r-1)+z}$, cujus aberratio ab exponente r utique major est, quam rationis $\frac{b}{a}=r+\frac{z}{a}$. Unde etiam facile intelligitur, si seriei a, b, c, d etc. plures termini a ratione geometrica $1:r$ aberrent, in serie differentiarum majores errores inesse debere.

2. **Corollarium.** Vicissim ergo quantumvis series differentiarum a proportione geometrica aberraverit, series terminorum ipsa propius ad hanc proportionem accedet.

3. **Propositio II.** Inter duos numeros datam rationem $1:r$ tenentes medium proportionalem invenire sine extractione radicis.

Solutio. Sint numeri propositi A et Ar, mediusque proportionalis prope saltem verus $=B$; ut hi tres numeri A, B, Ar progressionem a geometrica parum aberrantem constituant. Statuantur autem differentiae pro lubitu: $B-A=a$ et $Ar-B=b$, hincque colligitur $A(r-1)=a+b$ et $B(r-1)=ar+b$, ita ut sit

$$A=\frac{a+b}{r-1} \quad \text{et} \quad B=\frac{ar+b}{r-1};$$

nihil autem impedit quominus numeri A et B in ratione $1:r-1$ augeantur, ut in integris habeamus:

$$A=a+b \quad \text{et} \quad B=ar+b,$$

unde sumtis pro lubitu binis numeris a et b, hi tres numeri

$$a+b, \quad ar+b, \quad ar+br,$$

quorum primus est ad tertium in ratione data $1:r$, eo propius ad progressionem geometricam accedent, quo minus numerorum assumtorum a et b ratio a ratione $1:\sqrt{r}$ aberraverit; seu fractio $\frac{ar+b}{a+b}$ propius ad valorem $\sqrt{r}$ accedet, quam fractio $\frac{b}{a}$. Quo igitur valorem medii proportionalis

$\sqrt{r}$ inter 1 et r accuratius obtineamus, statuamus $a + b = a'$ et $ar + b = b'$; atque fractio $\frac{a'r + b'}{a' + b'}$ adhuc propius valorem $\sqrt{r}$ exhibebit. Simili ergo modo si porro statuamus

$$a' + b' = a'', \quad a'' + b'' = a''', \quad a''' + b''' = a^{IV} \text{ etc.}$$
$$a'r + b' = b'', \quad a''r + b'' = b''', \quad a'''r + b''' = b^{IV} \text{ etc.}$$

fractiones $\frac{b''}{a''}$, $\frac{b'''}{a'''}$, $\frac{b^{IV}}{a^{IV}}$ etc. continuo accuratius valorem medii proportionalis $\sqrt{r}$ exprimment.

4. **Coroll. 1.** Cum igitur quaestio sit de medio proportionali inter numeros $1:r$, sumtis pro lubitu duobus numeris a et b, formentur inde duae series

$$a, \quad a', \quad a'', \quad a''', \quad a^{IV} \text{ etc.}$$
$$b, \quad b', \quad b'', \quad b''', \quad b^{IV} \text{ etc.}$$

hac lege ut sit

$$a' = a + b, \quad a'' = a' + b', \quad a''' = a'' + b'', \quad a^{IV} = a''' + b'''$$
$$b' = ar + b, \quad b'' = a'r + b', \quad b''' = a''r + b'', \quad b^{IV} = a'''r + b'''$$

et fractiones $\frac{b}{a}$, $\frac{b'}{a'}$, $\frac{b''}{a''}$, $\frac{b'''}{a'''}$, $\frac{b^{IV}}{a^{IV}}$ etc. continuo propius valorem quaesitum $\sqrt{r}$ exhibebunt.

5. **Coroll. 2.** Vel si constituatur progressio a ratione geometrica continua quantumvis aberrans, cujus termini alterni sint in ratione $1:r$

$$a, \ b, \ ar, \ br, \ ar^2, \ br^2, \ ar^3, \ br^3, \ ar^4, \ br^4 \text{ etc.}$$

hinc binis terminis conjungendis nova formetur progressio:

$$a + b, \ b + ar, \ ar + br, \ br + ar^2, \ ar^2 + br^2, \ br^2 + ar^3, \text{ etc.}$$

haecque magis ad progressionem geometricam accedet.

6. **Coroll. 3.** Si hic denuo bini termini conjungantur, prodibit haec series:

$$a(r + 1) + 2b, \quad 2ar + b(r + 1), \quad ar(r + 1) + 2br, \quad 2ar^2 + br(r + 1) \text{ etc.}$$

hincque porro simili modo istae

$$a(3r + 1) + b(r + 3), \quad ar(r + 3) + b(3r + 1), \quad ar(3r + 1) + br(r + 3) \text{ etc.}$$
$$a(rr + 6r + 1) + b(4r + 4), \quad ar(4r + 4) + b(rr + 6r + 1), \quad ar(rr + 6r + 1) + br(4r + 4) \text{ etc.}$$
$$a(5rr + 10r + 1) + b(rr + 10r + 5), \quad ar(rr + 10r + 5) + b(5rr + 10r + 1) \text{ etc.}$$

quae continuo propius ad progressionem geometricam convergunt.

7. **Scholion.** Totum ergo negotium huc redit, ut binae series

$$a, \ a', \ a'', \ a''' \text{ etc.} \quad b, \ b', \ b'', \ b''', \ b^{IV} \text{ etc.}$$

formentur, quippe quarum termini homologi continuo propius rationem $1:\sqrt{r}$ exhibebunt. Cum autem singuli termini post primos utramque litteram a et b involvant, ita ut quilibet terminus utriusque hanc habiturus sit formam $Ma + Nb$, primum observo posteriorem seriem ex priori oriri, si loco litterarum a et b scribantur b et ar. Quare si prioris seriei terminus indici n respondens fuerit $a^{(n)} = Ma + Nb$, posterioris seriei terminus eidem indici n respondens erit $b^{(n)} = Mb + Nar$, ita ut fractio $\frac{Mb + Nar}{Ma + Nb}$ eo exactius valorem $\sqrt{r}$ sit expressura, quo major fuerit exponens n, atque adeo sumto $n = \infty$ verus valor $\sqrt{r}$ prodire debeat. Ita si exempli gratia capiatur $r = 2$, series illae binae ita se habebunt:

a	$a + b$	$3a + 2b$	$7a + 5b$	$17a + 12b$	$41a + 29b$
b	$2a + b$	$4a + 3b$	$10a + 7b$	$24a + 17b$	$58a + 41b$
$2a$	$2a + 2b$	$6a + 4b$	$14a + 10b$	$34a + 24b$	$82a + 58b$

cui tertiam subscripsi primae duplam, quippe cujus ope continuatio facillime instituitur. Quicunque ergo numeri hic pro a et b accipiantur, series media continebit satis prope media proportionalia inter primam et tertiam, uti facile perspicitur. Simili modo sumto $r = 3$, hae series ita se habebunt

a	$a + b$	$4a + 2b$	$10a + 6b$	$28a + 16b$	$76a + 44b$
b	$3a + b$	$6a + 4b$	$18a + 10b$	$48a + 28b$	$132a + 76b$
$3a$	$3a + 3b$	$12a + 6b$	$30a + 18b$	$84a + 48b$	$228a + 132b$

eritque ergo ex ultimis $\frac{132a + 76b}{76a + 44b} = \frac{33a + 19b}{19a + 11b}$ eo exactius $= \sqrt{3}$, quo propius ratio $\frac{b}{a}$ eo accedat, ita sumto $b = 2$ et $a = 1$ fit admodum exacte $\sqrt{3} = \frac{71}{41}$, et nunc sumto $b = 71$ et $a = 41$ exactissime erit $= \frac{2702}{1560} = \frac{1351}{780} = \sqrt{3}$ errore ne millionesimam quidem partem unitatis attingente.

8. **Propositio III.** Investigare legem progressionis binarum illarum serierum

$$a,\ a',\ a'',\ a'''\ \text{etc.}\quad \text{et}\quad b,\ b',\ b'',\ b'''\ \text{etc.},$$

quarum termini homologi continuo propius rationem $1 : \sqrt{r}$ exprimunt.

Solutio. Quoniam novimus omnes terminos binas litteras a et b ita complecti, ut in forma $Ma + Nb$ contineantur, ac si pro priori statuatur in genere $a^{(n)} = Ma + Nb$, tum pro posteriori fore $b^{(n)} = Mb + Nar$, hinc lex progressionis suppeditat terminos sequentes:

$$a^{(n+1)} = (M + Nr)\,a + (M + N)\,b \quad \text{et} \quad b^{(n+1)} = (M + Nr)\,b + (M + N)\,ra,$$

ex quo in legem progressionis utriusque seriei inquiri oportet. Quo igitur scrutemur, quemadmodum primae seriei quilibet terminus definiatur, consideremus hanc seriem sub ista forma generaliori

$$a + a'x^1 + a''x^2 + a'''x^3 + a^{IV}x^4 + \text{etc.}$$

cujus in infinitum continuatae summa fingatur $Pa + Qb$ et quoniam altera ex hac nascitur, dum loco a et b scribitur b et ra, erit

$$b + b'x + b''x^2 + b'''x^3 + b^{IV}x^4 + \text{etc.} = Pb + Qra.$$

Addantur hae series invicem, et quia est

$$a + b = a',\quad a' + b' = a'',\quad a'' + b'' = a'''\ \text{etc.}$$

erit $$a' + a''x + a'''x^2 + a^{IV}x^3 + \text{etc.} = (P + Qr)\,a + (P + Q)\,b.$$

Multiplicemus hanc seriem per x et a prima subtrahamus prodibitque

$$a = Pa + Qb - (P + Qr)\,ax - (P + Q)\,bx.$$

Quoniam vero quantitates P et Q a litteris a et b non pendent, hinc duae resultant aequationes

$$1 = P - Px - Qrx \quad \text{et} \quad 0 = Q - Px - Qx,$$

unde deducimus has determinationes:

$$P = \frac{1-x}{(1-x)^2 - rxx} = \frac{1-x}{1-2x-(r-1)xx}$$

et
$$Q = \frac{Px}{1-x} = \frac{x}{1-2x-(r-1)xx}.$$

Quocirca prior series $a + a'x + a''x^2 + a'''x^3 +$ etc. nascitur ex evolutione hujus fractionis $\frac{a(1-x)+bx}{1-2x-(r-1)xx}$, posterior vero $b + b'x + b''x^2 + b'''x^3 +$ etc. ex evolutione hujus $\frac{b(1-x)+arx}{1-2x-(r-1)xx}$, ita ut utraque sit series recurrens secundi ordinis, scala relationis existente 2, $(r-1)$, hincque pro serie priori a, a', a'', a''', a^{IV} etc. sit primo $a' = a + b$, tum vero $a'' = 2a' + (r-1)a$, $a''' = 2a'' + (r-1)a'$, $a^{IV} = 2a''' + (r-1)a''$ etc. ex hac vero nascitur altera ponendo $a = b$ et $b = ra$ Hinc adeo hujus seriei terminum generalem definire licet, ad quod valores quantitatum P et Q in fractiones simplices resolvi oportet. Cum igitur denominatoris communis factor sit

$$1 - x - x\sqrt{r} = 1 - x(1+\sqrt{r}),$$

pro quantitate P statuatur fractio simplex inde nata $= \frac{\mathfrak{A}}{1-x(1+\sqrt{r})}$, ac demonstravi fore $\mathfrak{A} = \frac{1-x}{1-x+x\sqrt{r}}$ posito $1 - x = x\sqrt{r}$, unde fit $\mathfrak{A} = \frac{1}{2}$; pro altero autem factore tantum $\sqrt{r}$ negative accipi opus est, ita ut sit

$$P = \frac{1}{2}\cdot\frac{1}{1-x(1+\sqrt{r})} + \frac{1}{2}\cdot\frac{1}{1-x(1-\sqrt{r})}.$$

Simili modo pro Q si fractio partialis ex denominatoris factore $1 - x(1+\sqrt{r})$ nata ponatur $\frac{\mathfrak{A}}{1-x(1+\sqrt{r})}$, reperietur $\mathfrak{A} = \frac{x}{1-x+x\sqrt{r}}$ posito $1 - x = x\sqrt{r}$, indeque $\mathfrak{A} = \frac{1}{2\sqrt{r}}$. Quare ipsi $\sqrt{r}$ binos valores tribuendo fit

$$Q = \frac{1}{2\sqrt{r}}\cdot\frac{1}{1-x(1+\sqrt{r})} - \frac{1}{2\sqrt{r}}\cdot\frac{1}{1-x(1-\sqrt{r})};$$

sicque summa prioris seriei $a + a'x + a''x^2 + a'''x^3 +$ etc., erit

$$= \frac{a\sqrt{r}+b}{2\sqrt{r}}\cdot\frac{1}{1-x(1+\sqrt{r})} + \frac{a\sqrt{r}-b}{2\sqrt{r}}\cdot\frac{1}{1-x(1-\sqrt{r})}.$$

Cum nunc ex utraque parte progressio nascatur geometrica, prodit nostrae seriei terminus generalis

$$\frac{a\sqrt{r}+b}{2\sqrt{r}}(1+\sqrt{r})^n x^n + \frac{a\sqrt{r}-b}{2\sqrt{r}}(1-\sqrt{r})^n x^n$$

ita ut sint indefinite

$$a^{(n)} = \frac{a\sqrt{r}+b}{2\sqrt{r}}(1+\sqrt{r})^n + \frac{a\sqrt{r}-b}{2\sqrt{r}}(1-\sqrt{r})^n,$$

et pro altera serie

$$b^{(n)} = \frac{b+a\sqrt{r}}{2}(1+\sqrt{r})^n + \frac{b-a\sqrt{r}}{2}(1-\sqrt{r})^n.$$

9. **Corollarium.** Ex hoc termino generali demum plene convincimur, fore sumto exponente n infinito, $\frac{b^{(n)}}{a^{(n)}} = \sqrt{r}$; cum enim tum potestas $(1-\sqrt{r})^n$ prae priori $(1+\sqrt{r})^n$ evanescat, erit utique

$$\frac{b^{(n)}}{a^{(n)}} = \frac{b\sqrt{r}+ar}{a\sqrt{r}+b} = \sqrt{r}.$$

Unde simul patet quo major capiatur exponens n, eo propius ad veritatem accedi.

10. **Scholion.** Eadem quidem veritas etiam hac ratione ostendi potest. Posito generatim $a^{(n)} = Ma + Nb$, erit $b^{(n)} = Mb + Nar$, et termini sequentes:

$$a^{(n+1)} = (M + Nr)\,a + (M + N)\,b \quad \text{et} \quad b^{(n+1)} = (M + Nr)\,b + (M + N)\,ar.$$

Jam casu $n = \infty$ nullum dubium superesse potest, quin sit $\frac{b^{(n+1)}}{a^{(n+1)}} = \frac{b^{(n)}}{a^{(n)}}$, unde necesse est sit:

$$\frac{(M + Nr)\,b + (M + N)\,ar}{(M + Nr)\,a + (M + N)\,b} = \frac{Mb + Nar}{Ma + Nb}.$$

Statuatur hic valor $= v$, et quia tum fit

$$\frac{M}{N} = \frac{bv - ar}{b - av} \quad \text{et} \quad \frac{M}{N} = \frac{arv + bv - br - ar}{b + ar - av - bv},$$

seu

$$\frac{M}{N} - v = \frac{a\,(vv - r)}{b - av} = \frac{(a + b)\,(vv - r)}{b + ar - (a + b)\,v},$$

unde manifesto sequitur $vv - r = 0$ et $v = \sqrt{r}$. Simul vero etiam quantitatum M et N haec relatio perspicitur, quod sumto $n = \infty$ fiat $\frac{M}{N} = v = \sqrt{r}$.

11. **Propositio IV.** Inter duos numeros datam rationem $1:r$ tenentes duos medios proportionales in rationalibus proxime exhibere.

Solutio. Sumantur bini numeri quicunque a et ar in ratione data, inter eosque capiantur duo medii quicunque b et c, atque quantumvis relatio $a:b:c:ar$ a ratione geometrica discrepet, inde alias propius eo accedentes hoc modo eliciemus. Quaerantur alii similes quaterni numeri $A:B:C:Ar$, quorum illi sint differentiae, ita ut sit $B - A = a$, $C - B = b$ et $Ar - C = c$, hincque $B = A + a$, $C = A + a + b$ et $Ar = A + a + b + c$, seu $A = \frac{a + b + c}{r - 1}$, $B = \frac{ar + b + c}{r - 1}$, $C = \frac{ar + br + c}{r - 1}$, qui per $r - 1$ multiplicati praebebunt hos quaternos numeros

$$a' = a + b + c, \quad b' = b + c + ar, \quad c' = c + ar + br, \quad a'r = ar + br + cr,$$

qui jam multo propius ad proportionem geometricam continuam accedent. Simili ergo modo hinc alii novi a'', b'', c'', $a''r$ derivabuntur sumendo:

$$a'' = a' + b' + c', \quad b'' = b' + c' + a'r, \quad c'' = c' + a'r + b'r$$

hincque denuo alii, qui continuo propius proposito satisfacient. Totum ergo negotium reducitur ad formationem trium progressionum:

$$\begin{array}{ll} \text{I.} & a,\ a',\ a'',\ a''',\ a^{IV} \ldots\ldots a^{(n)} \\ \text{II.} & b,\ b',\ b'',\ b''',\ b^{IV} \ldots\ldots b^{(n)} \\ \text{III.} & c,\ c',\ c'',\ c''',\ c^{IV} \ldots\ldots c^{(n)} \end{array}$$

quarum lex est satis simplex, quae quo ulterius continuentur, eo propius quaterni numeri

$$a^{(n)} : b^{(n)} : c^{(n)} : ra^{(n)}$$

proportionem geometricam continuam exhibebunt, etiamsi initio assumti a, b, c, ra plurimum aberraverint.

12. **Coroll. 1.** De his tribus seriebus primum observo singulos earum terminos hujusmodi formam $La + Mb + Nc$ esse habituros, ita ut quantitates L, M, N litteras pro arbitrio assumtas a, b, c non involvant, sed a sola ratione proposita $1:r$ pendeant.

13. **Coroll. 2.** Deinde si primae seriei terminus quicunque fuerit $a^{(n)} = La + Mb + Nc$, evidens est pro serie secunda fore $b^{(n)} = Lb + Mc + Nra$, et pro serie tertia $c^{(n)} = Lc + Mra + Nrb$. Unde sufficit harum trium serierum primae indolem exploravisse.

14. **Scholion.** Harum observationum ope inventio duarum mediarum proportionalium, quae quidem in rationalibus proxime satisfaciat, expedite instituitur. Sint enim exempli causa inter duos numeros rationem duplam tenentes duo medii proportionales investigandi, et operatio numerica sumendis pro litteris a, b, c numeris 1, 1, 1 ob $r = 2$ ita se habebit

a . . 1	3	12	46	177	681	2620	10080
b . . 1	4	15	58	223	858	3301	12700
c . . 1	5	19	73	281	1081	4159	16001
$2a$ . . 2	6	24	92	354	1362	5240	20160
$2b$ . . 2	8	30	116	446	1716	6602	25400

Hic quatuor postremi numeri

$$10080 : 12700 : 16001 : 20160$$

tam parum a proportione geometrica recedunt, ut si inter extremos per extractionem radicis cubicae duo medii proportionales quaerantur, ii ne parte quidem decies millesima a veritate aberrent; est enim

$$\frac{12700}{10080} = \sqrt[3]{\frac{2048383000}{1024192512}} = \sqrt[3]{\left(2 - \frac{2024}{1024192512}\right)}$$

ideoque $= \sqrt[3]{2} - \frac{2024}{3 . 1024192512 \sqrt[3]{4}}$, unde cum fiat $12700 = 10080 \sqrt[3]{2} - \frac{1}{23906}$, error infra particulam decies millesimam unitatis subsistit, ipsa autem fractio $\frac{12700}{10080}$ tantum particula $\frac{1}{10080 . 23906} = \frac{1}{24097248}$, hoc est minore quam vicies millionesima unitatis a vero valore $\sqrt[3]{2}$ deficit, tantam autem praecisionem ope logarithmorum attingere non licet. Unde intelligitur, quantum usum haec methodus praestare queat in radicibus cujusvis dignitatis proxime exprimendis.

15. **Propositio V.** Investigare legem harum trium progressionum:

$$a, a', a'' \text{ etc.} \quad b, b', b'' \text{ etc.} \quad c, c', c'' \text{ etc.}$$

quarum termini homologi $a^{(n)} : b^{(n)} : c^{(n)}$ continuo propius proportionem $1 : \sqrt[3]{r} : \sqrt[3]{r^2}$ exprimunt.

Solutio. Cum omnes termini ex ternis primo assumtis a, b et c ita componantur, ut sit $a^{(n)} = La + Mb + Nc$, erit ex earum indole $b^{(n)} = Lb + Mc + Nra$ et $c^{(n)} = Lc + Mra + Nrb$, at lex progressionis praebet sequentes terminos:

$$a^{(n+1)} = (L + Mr + Nr)\, a + (L + M + Nr)\, b + (L + M + N)\, c$$
$$b^{(n+1)} = (L + Mr + Nr)\, b + (L + M + Nr)\, c + (L + M + N)\, ra$$
$$c^{(n+1)} = (L + Mr + Nr)\, c + (L + M + Nr) ra + (L + M + N)\, rb.$$

Hinc si generalius statuamus:

$$a + a'x + a''x^2 + a'''x^3 + \text{etc.} = Pa + Qb + Rc,$$

erit
$$b + b'x + b''x^2 + b'''x^3 + \text{etc.} = Pb + Qc + Rra,$$
$$c + c'x + c''x^2 + c'''x^3 + \text{etc.} = Pc + Qra + Rrb.$$

Addantur hae series invicem, et quia est

$$a + b + c = a',\ a' + b' + c' = a'',\quad a'' + b'' + c'' = a''',$$

erit $\quad a' + a''x + a'''x^2 + \text{etc.} = (P + Qr + Rr)\,a + (P + Q + Rr)\,b + (P + Q + R)\,c,$

quae per x multiplicata et a prima subtracta dat

$$a = Pa + Qb + Rc - (P + Qr + Rr)\,ax - (P + Q + Rr)\,bx - (P + Q + R)\,cx.$$

Quia autem quantitates P, Q, R litteras a, b, c non involvunt, hinc nascuntur tres aequationes:

$$\left.\begin{array}{ll} \text{I.} & 1 = P - Px - Qrx - Rrx \\ \text{II.} & 0 = Q - Px - Qx - Rrx \\ \text{III.} & 0 = R - Px - Qx - Rx \end{array}\right\} \quad \text{hincque} \quad \left\{\begin{array}{l} 1 = P - Q - Q(r-1)\,x \\ 0 = Q - R - R(r-1)\,x \\ 1 = P - R - (Q + R)(r-1)\,x. \end{array}\right.$$

Pro faciliori resolutione statuamus $1 - x + rx = z$, et sequens combinatio praebebit

$$\left.\begin{array}{ll} \text{I} - \text{II}. & 1 = P - Qz \\ \text{II} - \text{III}. & 0 = Q - Rz \end{array}\right\} \quad \text{hinc} \quad \left\{\begin{array}{l} Q = Rz \\ P = 1 + Rzz, \end{array}\right.$$

unde fit

$$\text{III.}\quad 0 = R(1 - x) - Px - Qx = R(1 - x - xz - xzz) - x,$$

ideoque

$$R = \frac{x}{1 - x(1 + z + zz)},\quad \text{at est}\quad x = \frac{z-1}{r-1},$$

ergo

$$R = \frac{z-1}{r - 1 - (z-1)(1 + z + zz)} = \frac{z-1}{r - z^3}$$

sicque prodit

$$P = \frac{r - zz}{r - z^3},\quad Q = \frac{zz - z}{r - z^3},\quad R = \frac{z-1}{r - z^3},$$

quarum formarum cum denominator sit

$$r - 1 - 3(r-1)\,x - 3(r-1)^2x^2 - (r-1)^3x^3,$$

seu
$$(r-1)(1 - 3x - 3(r-1)\,x^2 - (r-1)^2x^3),$$

perspicuum est nostras tres progressiones esse recurrentes, scala relationis existente 3, $3(r-1)$, $(r-1)^2$, ita ut sit

$$a^{(n)} = 3a^{(n-1)} + 3(r-1)\,a^{(n-2)} + (r-1)^2a^{(n-3)}.$$

Nunc pro terminis generalibus harum progressionum fractiones P, Q, R in simplices resolvi oportet: quoniam autem denominatoris factor simplex est $\sqrt[3]{r} - z$ simul vicem binorum reliquorum gerens, siquidem $\sqrt[3]{r}$ tres involvit valores diversos, sufficit hunc unicum factorem considerasse. Sit ergo ex fractione R fractio simplex oriunda $= \frac{A}{\sqrt[3]{r} - z}$, et numerator erit $A = \frac{z-1}{\sqrt[3]{rr} + z\sqrt[3]{r} + zz}$ posito $z = \sqrt[3]{r}$, unde fit $A = \frac{\sqrt[3]{r} - 1}{3\sqrt[3]{rr}}$, ideoque

$$P = \frac{1}{3\sqrt[3]{r^2}} \cdot \frac{r - \sqrt[3]{r^2}}{\sqrt[3]{r} - z} + \text{etc.}, \quad Q = \frac{1}{3\sqrt[3]{r^2}} \cdot \frac{\sqrt[3]{r^2} - \sqrt[3]{r}}{\sqrt[3]{r} - z} + \text{etc.}, \quad R = \frac{1}{3\sqrt[3]{r^2}} \cdot \frac{\sqrt[3]{r} - 1}{\sqrt[3]{r} - z} + \text{etc.}$$

Restituatur pro z valor $1 + (r - 1)x$, sitque $\frac{r-1}{\sqrt[3]{r} - 1} = s$, ac fiet

$$P = \frac{1}{3} \cdot \frac{1}{1 - sx} + \text{etc.}, \quad Q = \frac{1}{3\sqrt[3]{r}} \cdot \frac{1}{1 - sx} + \text{etc.}, \quad R = \frac{1}{3\sqrt[3]{r^2}} \cdot \frac{1}{1 - sx} + \text{etc.}$$

Hinc cum sit $a + a'x + a''x^2 + \text{etc.} = Pa + Qb + Rc$, sequitur fore

$$a^{(n)} = \frac{1}{3} s^n \left(a + \frac{b}{\sqrt[3]{r}} + \frac{c}{\sqrt[3]{rr}}\right) + \cdots\cdot + \cdots\cdot$$

ubi duo membra omissa ex primo ita formantur, ut loco $\sqrt[3]{r}$ scribatur $\frac{-1 \pm \sqrt{-3}}{2} \sqrt[3]{r}$, id quod etiam de $s = \frac{r-1}{\sqrt[3]{r} - 1}$ est intelligendum. Deinde vero pro binis reliquis seriebus habebitur:

$$b^{(n)} = \frac{1}{3} s^n \left(a\sqrt[3]{r} + b + \frac{c}{\sqrt[3]{r}}\right) + \cdots\cdot + \cdots\cdot$$

$$c^{(n)} = \frac{1}{3} s^n (a\sqrt[3]{r^2} + b\sqrt[3]{r} + c) + \cdots\cdot + \cdots\cdot$$

16. **Coroll. 1.** Si n sit numerus praegrandis, bina membra omissa prae primis hic appositis evanescunt; ex quo perspicuum est tum fore

$$a^{(n)} : b^{(n)} : c^{(n)} = 1 : \sqrt[3]{r} : \sqrt[3]{rr};$$

in quo ipso tota vis methodi hic traditae consistit.

17. **Coroll. 2.** Natura harum serierum recurrentium tertii ordinis ideo imprimis notari meretur, quod fractiones principales P, Q, R tam concinne in fractiones simplices resolvere licuit; atque ex terminis generalibus inde derivatis natura harum serierum facile perspicitur.

18. **Scholion.** Hinc ratio istam methodum ad plures medias proportionales extendendi ita jam est manifesta, ut superfluum foret omnia ratiocinia, quibus operationes usurpatae innituntur, repetere. Quamobrem inventionem plurium mediarum proportionalium inter duos numeros datam rationem $1:r$ tenentes, nunc quidem satis succincte exponere atque adeo binas propositiones cuique casui tribuendas commode in unam contrahere poterimus.

19. **Propositio VI.** Inter duos numeros rationem datam $1:r$ tenentes, tres medias continue proportionales in rationalibus proxime exhibere.

Solutio. Sumtis in ratione data duobus numeris a et ra, inter eos pro lubitu tres medii constituantur b, c, d, ut habeantur hi quinque numeri quantumvis a scopo aberrantes:

$$a : b : c : d : ra.$$

Hinc formentur alii hac lege ut sit

$$\begin{aligned} a' &= a + b + c + d \\ b' &= b + c + d + ra \\ c' &= c + d + ra + rb \\ d' &= d + ra + rb + rc \end{aligned}$$

qui constituent progressionem jam multo propius ad scopum attingentem hanc:

$$a' : b' : c' : d' : ra',$$

ex quibus porro eadem lege alii novi quaerantur, indeque denuo alii, quo pacto continuo propius ad proportionem geometricam continuam accedetur, ita ut abberratio tandem omni assignabili minor evadat. Singulae porro harum serierum

$$a,\ a',\ a'',\ a''',\ a^{IV} \text{ etc.}$$
$$b,\ b',\ b'',\ b''',\ b^{IV} \text{ etc.}$$
$$c,\ c',\ c'',\ c''',\ c^{IV} \text{ etc.}$$
$$d,\ d',\ d'',\ d''',\ d^{IV} \text{ etc.}$$

sunt recurrentes quarti ordinis secundum scalam relationis:

$$4,\ 6(r-1),\ 4(r-1)^2,\ (r-1)^3.$$

Denique harum serierum termini generales, posito brevitatis gratia

$$\frac{r-1}{\sqrt[4]{r}-1} = 1 + \sqrt[4]{r} + \sqrt[4]{r^2} + \sqrt[4]{r^3} = s$$

erunt

$$a^{(n)} = \frac{a\sqrt[4]{r^3} + b\sqrt[4]{r^2} + c\sqrt[4]{r} + d}{4\sqrt[4]{r^3}} s^n + \text{etc.}$$

$$b^{(n)} = \frac{a\sqrt[4]{r^3} + b\sqrt[4]{r^2} + c\sqrt[4]{r} + d}{4\sqrt[4]{r^2}} s^n + \text{etc.}$$

$$c^{(n)} = \frac{a\sqrt[4]{r^3} + b\sqrt[4]{r^2} + c\sqrt[4]{r} + d}{4\sqrt[4]{r}} s^n + \text{etc.}$$

$$d^{(n)} = \frac{a\sqrt[4]{r^3} + b\sqrt[4]{r^2} + c\sqrt[4]{r} + d}{4} s^n + \text{etc.}$$

quarum expressionum prima tantum membra apposui, dum ex his reliqua facile formantur, loco $\sqrt[4]{r}$ ejus ternos reliquos valores substituendo. Ceterum si statuatur

$$a + a'x + a''x^2 + a'''x^3 + a^{IV}x^4 + \text{etc.} = Pa + Qb + Rc + Sd$$

ac brevitatis gratia fiat $1 - x + rx = z$, reperitur ut ante:

$$P = \frac{r - z^3}{r - z^4};\quad Q = \frac{z^3 - z^2}{r - z^4};\quad R = \frac{z^2 - z}{r - z^4};\quad S = \frac{z - 1}{r - z^4};$$

unde simul reliquarum similium serierum a litteris b, c, d incipientium summae exhibentur.

20. **Exemplum.** Inter duos numeros rationem duplam tenentes, tres medii proportionales sequenti modo reperiuntur:

a ... 1	4	22	116	613	3240	17124	90504
b ... 1	5	26	138	729	3853	20364	107628
c ... 1	6	31	164	867	4582	24217	127992
d ... 1	7	37	195	1031	5449	28799	152209
$2a$ ... 2	8	44	232	1226	6480	34248	181008

ubi ultimi numeri tam prope progressionem geometricam in ratione $1 : \sqrt[4]{2}$ procedentem constituunt,

quam fieri potest, numeris non majoribus adhibendis. Ita satis exacte erit $\frac{107628}{90504} = \sqrt[4]{2}$, seu per 12 reducendo $\frac{8969}{7542} = \sqrt[4]{2}$, cujus error longe infra partem millionesimam unitatis subsistit.

21. **Scholion 1.** In Musicis similis quaestio de undecim mediis proportionalibus inter rationem duplam inveniendis tractari solet, ut hinc omnia semitonia unius *Octavae* inter se aequalia reddantur; quod temperamentum etsi principiis harmoniae adversatur, tamen non abs re fore arbitror ejus solutionem ex iisdem principiis petitam hic apponere:

A . . 1	12	210	3532	59379	998592
B . . 1	13	222	3742	62911	1057971
H . . 1	14	235	3964	66653	1120882
C . . 1	15	249	4199	70617	1187535
Cs. . 1	16	264	4448	74816	1258152
D . . 1	17	280	4712	79264	1332968
Ds. . 1	18	297	4992	83976	1412232
E . . 1	19	315	5289	88968	1496208
F . . 1	20	334	5604	94257	1585176
Fs. . 1	21	354	5938	99861	1679433
G . . 1	22	375	6292	105799	1779294
Gs . . 1	23	397	6667	112091	1885093
a . . 2	24	420	7064	118758	1997184

ultima columna tam parum a progressione geometrica recedit, ut error ne ad millionesimam partem assurgere sit censendus.

22. **Scholion 2.** Quae hactenus sunt tradita facile ad quotcunque medios proportionales inveniendos in genere accommodari possunt, in quo negotio hoc imprimis notari meretur, quod series numerorum, quibus solutio continetur, non solum sint recurrentes, sed etiam denominator fractionum, ex quibus nascuntur, semper in factores resolvi queat, ad quemcunque etiam gradum ascendat: unde egregia exempla aequationum altioris gradus solutionem admittentium colliguntur, quibus conjectura mea circa formam radicum cujusque gradus olim prolata pulcherrime confirmatur. Verum methodus hic exposita multo latius extendi potest, quemadmodum in sequente propositione sum ostensurus: ita ut inde adhuc majora subsidia in analysin redundatura videantur.

23. **Propositio VII.** Methodum multo latius patentem exhibere, cujus ope inter duos numeros datam rationem $1:r$ tenentes quotcunque medii proportionales in rationalibus proxime inveniri queant.

Solutio. Inter duos numeros a et ar datam rationem tenentes ut ante totidem medii pro lubitu accipiantur, quot medios proportionales assignari oportet. Ponamus autem quatuor medios inveniri debere, quoniam hinc vis methodi clarius perspicietur, quam si rem generaliter tractare velimus. Constituta ergo pro hoc casu ad lubitum tali progressione

$$a:b:c:d:e:ar:br:cr:dr:er:ar^2 \text{ etc.}$$

sumantur pro arbitrio quinque indices α, β, γ, δ, ε, per quos inde nova similis progressio formetur:

$$a':b':c':d':e':a'r:b'r:c'r:d'r:e'r:a'r^2 \text{ etc.}$$

hac lege ut sit

$$\begin{aligned}
a' &= \alpha a + \beta b + \gamma c + \delta d + \varepsilon e\\
b' &= \alpha b + \beta c + \gamma d + \delta e + \varepsilon ar\\
c' &= \alpha c + \beta d + \gamma e + \delta ar + \varepsilon br\\
d' &= \alpha d + \beta e + \gamma ar + \delta br + \varepsilon cr\\
e' &= \alpha e + \beta ar + \gamma br + \delta cr + \varepsilon dr.
\end{aligned}$$

Tum vero per eosdem indices ex hac progressione denuo alia formetur nova, atque ita porro; ut hac ratione sequentes series obtineantur

$$\begin{aligned}
a + a'x + a''x^2 + a'''x^3 + \text{etc.} &= Pa + Qb + Rc + Sd + Te\\
b + b'x + b''x^2 + b'''x^3 + \text{etc.} &= Pb + Qc + Rd + Se + Tar\\
c + c'x + c''x^2 + c'''x^3 + \text{etc.} &= Pc + Qd + Re + Sar + Tbr\\
d + d'x + d''x^2 + d'''x^3 + \text{etc.} &= Pd + Qe + Rar + Sbr + Tcr\\
e + e'x + e''x^2 + e'''x^3 + \text{etc.} &= Pe + Qar + Rbr + Scr + Tdr
\end{aligned}$$

unde ex lege praescripta valores litterarum P, Q, R, S, T quae a litteris arbitrariis a, b, c, d, e sunt immunes, et tantum ab indicibus α, β, γ, δ, ε una cum quantitate x et ratione proposita $1:r$ pendent, ita determinantur ut sit:

$$\begin{aligned}
\frac{P-1}{x} &= \alpha P + \beta Tr + \gamma Sr + \delta Rr + \varepsilon Qr\\
\frac{Q}{x} &= \alpha Q + \beta P + \gamma Tr + \delta Sr + \varepsilon Rr\\
\frac{R}{x} &= \alpha R + \beta Q + \gamma P + \delta Tr + \varepsilon Sr\\
\frac{S}{x} &= \alpha S + \beta R + \gamma Q + \delta P + \varepsilon Tr\\
\frac{T}{x} &= \alpha T + \beta S + \gamma R + \delta Q + \varepsilon P
\end{aligned}$$

ex quibus aequalitatibus quidem valores harum litterarum admodum perplexi eliciuntur, ita ut denominator communis hujusmodi formam sit habiturus:

$$1 - Ax - Bx^2 - Cx^3 - Dx^4 - Ex^5$$

indicium praebens series illas esse recurrentes, ex eadem scala relationis oriundas. Verum quod hic potissimum est notandum, hunc denominatorem semper in factores simplices resolvere licet, qui inter se ita erunt similes, ut ex quinis ipsius $\sqrt[5]{r}$ valoribus simili modo formentur. Scilicet si brevitatis gratia ponatur

$$\alpha + \beta\sqrt[5]{r} + \gamma\sqrt[5]{r^2} + \delta\sqrt[5]{r^3} + \varepsilon\sqrt[5]{r^4} = s$$

ubi etiam s quinos valores diversos sortitur, erit $1 - sx$ factor simplex illius denominatoris, simul omnes quinque in se involvens. Hinc ergo singulas fractiones, quibus litterae illae P, Q, R, S, T exprimuntur, in quinque fractiones simplices resolvere licebit, quae ita concinne expressae reperiuntur:

$$P = \frac{1}{5(1-sx)} + \cdots + \cdots + \cdots + \cdots$$

$$Q = \frac{1}{5(1-sx)\sqrt[5]{r}} + \cdots + \cdots + \cdots + \cdots$$

$$R = \frac{1}{5(1-sx)\sqrt[5]{r^2}} + \cdots + \cdots + \cdots + \cdots$$

$$S = \frac{1}{5(1-sx)\sqrt[5]{r^3}} + \cdots + \cdots + \cdots + \cdots$$

$$T = \frac{1}{5(1-sx)\sqrt[5]{r^4}} + \cdots + \cdots + \cdots + \cdots$$

ubi quaterna membra punctis indicata ex primis, ipsi $\sqrt[5]{r}$ quatuor reliquos valores tribuendo, sunt supplenda.

Hinc jam quinque serierum a numeris arbitrariis a, b, c, d, e incipientium termini generales formari possunt, qui etiam ponendo brevitatis gratia

$$a\sqrt[5]{r^4} + b\sqrt[5]{r^3} + c\sqrt[5]{r^2} + d\sqrt[5]{r} + e = k,$$

(ubi quoque quantitas k quinque valores involvere est existimanda) sequenti modo concinne exprimuntur:

$$a^{(n)} = \frac{k}{5\sqrt[5]{r^4}}s^n + \cdots + \cdots + \cdots + \cdots$$

$$b^{(n)} = \frac{k}{5\sqrt[5]{r^3}}s^n + \cdots + \cdots + \cdots + \cdots$$

$$c^{(n)} = \frac{k}{5\sqrt[5]{r^2}}s^n + \cdots + \cdots + \cdots + \cdots$$

$$d^{(n)} = \frac{k}{5\sqrt[5]{r}}s^n + \cdots + \cdots + \cdots + \cdots$$

$$e^{(n)} = \frac{k}{5}s^n + \cdots + \cdots + \cdots + \cdots$$

ubi quaterna membra omissa simili modo ut supra ex primis constitui oportet.

Hinc jam id, in quo cardo rei versatur, intelligitur: scilicet si series illae in infinitum continuentur, ut exponens n in infinitum excrescat, tum respectu ejus membri, in quo ipsi $\sqrt[5]{r}$ valor realis positivus tribuitur, reliqua evanescere, sicque manifesto numeros $a^{(n)}:b^{(n)}:c^{(n)}:d^{(n)}:e^{(n)}:ra^{(n)}$ progressionem geometricam constituere. Verum hic probe est notandum, illam evanescentiam locum non habere nisi indices α, β, γ, δ, ε sint positivi, quemadmodum hinc etiam casus supra tractatus resultat, si hi indices unitati aequales statuantur.

24. **Scholion.** Circa hanc solutionem generalem observari convenit, quod si valores litterarum P, Q, R, S, T ex formulis inventis evolvantur, earumque denominator communis ad nihilum redigatur, ut posito $x = \frac{1}{z}$ hujusmodi prodeat aequatio quinti gradus:

$$z^5 - Az^4 - Bz^3 - Cz^2 - Dz - E = 0$$

tum hujus aequationis radicem fore

$$z = \alpha + \beta\sqrt[5]{r} + \gamma\sqrt[5]{r^2} + \delta\sqrt[5]{r^3} + \varepsilon\sqrt[5]{r^4},$$

in qua forma simul omnes quinque radices contineantur, si modo pro $\sqrt[5]{r}$ ejus quinque valores successive substituantur. Cum igitur hae radices eam ipsam habeant formam, quam olim conjectura eram assecutus, hinc multo confidentius affirmare poterimus, omnium aequationum cujuscunque gradus radices eo modo exprimi, quem conjectura mea indicat. Quodsi indices α, β, γ, δ, ε unitati aequentur, aequatio quinti gradus fit ex superioribus:

$$z^5 - 5z^4 - 10(r-1)z^3 - 10(r-1)^2 z^2 - 5(r-1)^3 z - (r-1)^4 = 0,$$

cujus radix erit

$$z = 1 + \sqrt[5]{r} + \sqrt[5]{r^2} + \sqrt[5]{r^3} + \sqrt[5]{r^4}.$$

Seu posito $z = y + 1$ erit hujus aequationis

$$y^5 = 10ry^3 + 10r(r+1)y^2 + 5r(rr+r+1)y + r(r^3+r^2+r+1)$$

radix

$$y = \sqrt[5]{r} + \sqrt[5]{r^2} + \sqrt[5]{r^3} + \sqrt[5]{r^4}.$$



XXIX.

Solutio problematis, quo duo quaeruntur numeri, quorum productum tam summa, quam differentia eorum, sive auctum sive minutum, fiat quadratum.

(N. Comment. XV. 1770. p. 29. Exhib. 1770 Mart. 5.)

1. Problema hoc mihi ante complures annos Berolini a Centurione quodam Prussico erat propositum, quod se Lipsiae ab amico accepisse ajebat; neque vero se neque istum amicum solutionem ullo modo invenire potuisse. Quaerebat igitur ex me, utrum hoc problema possibile judicarem, nec ne? Statim quidem hoc problema mihi ob elegantiam mirifice placebat, et quum facile summam solutionis difficultatem perspexissem, id omnino dignum judicavi in quo vires meas exercerem. Tandem vero post plura tentamina solutionem sum adeptus, quae ita se habebat: Positis duobus numeris quaesitis A et B, inveni

$$A = \frac{13.29^2}{8.9^2} = \frac{10933}{648} \quad \text{et} \quad B = \frac{5.29^2}{32.11^2} = \frac{4205}{3872}.$$

2. Via autem, qua ad hanc solutionem perveni, ita erat comparata, ut nullo modo mihi liceret, alias solutiones inde eruere; etiamsi nullus dubitandi locus relinqueretur, quin hoc problema innumerabiles admitteret solutiones. Nuper autem cum in hoc idem argumentum incidissem, casu prorsus fortuito methodus mihi se obtulit, infinitas solutiones hujus problematis eliciendi. Quod quum casui prorsus singulari sit acceptum referendum, quaestio haec omnino digna mihi est visa, quam accuratius perscrutarer. Quare primo quidem solutionem generalem proponam, deinde vero artificium illud, quod mihi infinitas solutiones suppeditavit, uberius evolvam.

Solutio problematis generalis.

3. Si litterae A et B denotent ambos numeros quaesitos, necesse est, ut sequentes quatuor formulae quadrata efficiantur:

$$\text{I.} \quad AB + A + B = \square; \qquad \text{II.} \quad AB + A - B = \square;$$
$$\text{III.} \quad AB - A + B = \square; \qquad \text{IV.} \quad AB - A - B = \square.$$

Quum autem statim pateat, hos numeros integros esse non posse, ob rationes mox perspiciendas, eos ita expressos assumo, ut sit $A = \frac{z}{x}$ et $B = \frac{z}{y}$, ita ut quatuor sequentes formulae ad quadrata reducendae habeantur:

$$\text{I.} \quad \frac{z}{xy}(z + y + x) = \square; \qquad \text{II.} \quad \frac{z}{xy}(z + y - x) = \square;$$
$$\text{III.} \quad \frac{z}{xy}(z - y + x) = \square; \qquad \text{IV.} \quad \frac{z}{xy}(z - y - x) = \square;$$

4. Quod si ergo factor communis fuerit quadratum, quatuor sequentes formulas quadrata effici oportet, quas quidem per ambiguitatem signorum ita duabus formulis comprehendere licet:

$$\text{I. et II.}\quad z+y\pm x=\square;\qquad \text{III. et IV.}\quad z-y\pm x=\square.$$

Quare quum in genere sit $aa+bb\pm 2ab=\square$ similique modo $cc+dd\pm 2cd=\square$; statuamus ut sequitur:

$$z+y=aa+bb;\quad x=2ab$$
$$z-y=cc+dd;\quad x=2cd.$$

Ut autem fiat $2ab=2cd$, statuatur utrumque $=2pqrs=x$, sumaturque $a=pq$, $b=rs$, $c=pr$ et $d=qs$, eritque

$$z+y=aa+bb=ppqq+rrss$$
$$z-y=cc+dd=pprr+qqss,$$

unde colligitur

$$z=\frac{(pp+ss)(qq+rr)}{2}\quad\text{et}\quad y=\frac{(pp-ss)(qq-rr)}{2}$$

tum vero erit

$$\text{I.}\quad z+y+x=(a+b)^2=(pq+rs)^2$$
$$\text{II.}\quad z+y-x=(a-b)^2=(pq-rs)^2$$
$$\text{III.}\quad z-y+x=(c+d)^2=(pr+qs)^2$$
$$\text{IV.}\quad z-y-x=(c-d)^2=(pr-qs)^2.$$

5. Superest igitur, ut etiam factor communis $\frac{z}{xy}$ quadratum reddatur, qui evolutus praebet hanc formulam:

$$\frac{z}{xy}=\frac{(pp+ss)(qq+rr)}{2pqrs(pp-ss)(qq-rr)}$$

at vero in hoc efficiendo summa consistit difficultas; quodsi enim numerator in denominatorem ducatur, ut haec formula quadratum fieri debeat:

$$2pqrs(pp-ss)(qq-rr)(pp+ss)(qq+rr)=\square$$

singulae litterae ad quinque dimensiones assurgunt, cujusmodi quaestiones in analysi Diophantea adhuc non sunt tractari solitae; ceterum jam olim post plura tentamina reperi huic conditioni satisfieri, sumendo $p=13$, $s=11$, $q=16$ et $r=11$, uti periculum facienti mox patebit.

6. Quodsi autem quocunque modo hujusmodi valores idonei pro litteris p, q, r, s fuerint inventi, solutio problematis inde ita adstruitur:

Posita formula $\frac{(pp+ss)(qq+rr)}{2pqrs(pp-ss)(qq-rr)}=\frac{M^2}{N^2}$, primo ambo numeri quaesiti ita erunt expressi

$$A=\frac{(pp+ss)(qq+rr)}{4pqrs}\quad\text{et}\quad B=\frac{(pp+ss)(qq+rr)}{(pp-ss)(qq-rr)}$$

tum vero conditionibus problematis ita satisfiet, ut sit

$$\text{I.}\quad \sqrt{(AB+A+B)}=\frac{M}{N}(pq+rs)$$

$$\text{II.}\quad \sqrt{(AB+A-B)}=\frac{M}{N}(pq-rs)$$

$$\text{III.}\quad \sqrt{(AB - A + B)} = \frac{M}{N}(pr + qs)$$

$$\text{IV.}\quad \sqrt{(AB - A - B)} = \frac{M}{N}(pr - qs).$$

Singularis evolutio nostrae formulae, quae ad quadratum est revocanda.

7. Quum omnis opera in hac formula reducenda frustra consumatur, quamdiu in ea tot diversae quantitates occurrunt, earumque singulae ad tot dimensiones assurgunt, ante omnia elaborandum est, ut diversis factoribus denominatoris communes divisores concilientur; hunc in finem usus sum sequentibus positionibus:

$$p + s = \alpha\beta,\quad p - s = \varepsilon\zeta,\quad q + r = \alpha\gamma \quad\text{et}\quad q - r = \varepsilon\eta,$$

ita ut fiat

$$p = \frac{\alpha\beta + \varepsilon\zeta}{2},\quad s = \frac{\alpha\beta - \varepsilon\zeta}{2},\quad q = \frac{\alpha\gamma + \varepsilon\eta}{2} \quad\text{et}\quad r = \frac{\alpha\gamma - \varepsilon\eta}{2},$$

tum vero nostra conditio principalis postulat, ut sit:

$$\frac{(pp + ss)(qq + rr)}{2pqrs.\beta\gamma\zeta\eta.\alpha^2\varepsilon^2} = \frac{M^2}{N^2} \quad\text{sive}\quad \frac{(pp + ss)(qq + rr)}{2pqrs.\beta\gamma\zeta\eta} = \frac{M^2}{N^2}.\alpha^2\varepsilon^2.$$

8. Secundo constituatur ratio inter litteras r et s, quae sit ut $f:g$, eritque

$$f:g :: \alpha\gamma - \varepsilon\eta : \alpha\beta - \varepsilon\zeta,\quad\text{sive}\quad g(\alpha\gamma - \varepsilon\eta) = f(\alpha\beta - \varepsilon\zeta),$$

unde colligitur $\alpha(f\beta - g\gamma) = \varepsilon(f\zeta - g\eta)$, quocirca ponamus: $\alpha = f\zeta - g\eta$, $\varepsilon = f\beta - g\gamma$; tum vero habebitur

$$p = \frac{2f\beta\zeta - g\beta\eta - g\gamma\zeta}{2},\quad q = \frac{f\beta\eta + f\gamma\zeta - 2g\gamma\eta}{2},\quad r = \frac{f(\gamma\zeta - \beta\eta)}{2} \quad\text{et}\quad s = \frac{g(\gamma\zeta - \beta\eta)}{2}.$$

9. Ut adhuc plures factores in denominatore communes reddamus; faciamus insuper $q = h\beta\zeta$, unde haec aequatio emergit:

$$2h\beta\zeta = f\beta\eta + f\gamma\zeta - 2g\gamma\eta,\quad\text{sive}\quad \beta(2h\zeta - f\eta) = \gamma(f\zeta - 2g\eta),$$

quamobrem ponamus

$$\beta = f\zeta - 2g\eta \quad\text{et}\quad \gamma = 2h\zeta - f\eta.$$

Ex his autem valoribus porro colligimus:

$$\alpha = f\zeta - g\eta,\qquad \varepsilon = (ff - 2gh)\zeta - fg\eta,$$
$$p + s = (f\zeta - g\eta)(f\zeta - 2g\eta) = ff\zeta\zeta - 3fg\zeta\eta + 2gg\eta\eta,$$
$$p - s = \zeta((ff - 2gh)\zeta - fg\eta) = (ff - 2gh)\zeta\zeta - fg\zeta\eta,$$
$$q + r = (f\zeta - g\eta)(2h\zeta - f\eta) = 2fh\zeta\zeta - (ff + 2hg)\zeta\eta + fg\eta\eta,$$
$$q - r = \eta((ff - 2gh)\zeta - fg\eta) = (ff - 2hg)\zeta\eta - fg\eta\eta,$$

hincque porro:

$$p = (ff - gh)\zeta\zeta - 2fg\zeta\eta + gg\eta\eta,$$
$$s = gh\zeta\zeta - fg\zeta\eta + gg\eta\eta = g(h\zeta\zeta - f\zeta\eta + g\eta\eta),$$
$$q = fh\zeta\zeta - 2gh\zeta\eta = h\zeta(f\zeta - 2g\eta),$$
$$r = fh\zeta\zeta - ff\zeta\eta + fg\eta\eta = f(h\zeta\zeta - f\zeta\eta + g\eta\eta).$$

10. Denique hos valores ita determinemus, ut numerus p divisor evadat formulae $qq + rr$, jam vero invenitur:

$$qq + rr = ffgg\eta^4 - 2f^3g\eta^3\zeta + (f^4 + 2ffgh + 4gghh)\,\eta\eta\zeta\zeta - 2fh\,(ff + 2gh)\,\eta\zeta^3 + 2ffhh\zeta^4$$

quare quum sit $p = gg\eta\eta - 2fg\eta\zeta + (ff - gh)\,\zeta\zeta$, ut p fiat factor illius formulae, statuatur alter factor $ff\eta\eta + t\zeta\eta + u\zeta\zeta$, eritque productum:

$$\begin{array}{l} ffgg\eta^4 - 2f^3g \\ \qquad\quad + tgg \end{array}\left.\right\}\eta^3\zeta + \left.\begin{array}{l}(f^4 - ffgh) \\ \quad - 2tfg \\ \quad + ugg\end{array}\right\}\eta\eta\zeta\zeta + \left.\begin{array}{l}t\,(ff - gh) \\ \quad - 2ufg\end{array}\right\}\eta\zeta^3 + u\,(ff - gh)\,\zeta^4$$

ubi primi termini jam congruunt, secundi vero dant $t = 0$, tertii $3ffgh + 4gghh = ugg$, unde $u = \frac{3ffh}{g} + 4hh$; quarti porro praebent $u = \frac{h(ff + 2gh)}{g}$; quinti vero tandem dant $u = \frac{2ffhh}{ff - gh}$. Necesse igitur est, ut hi tres valores ipsius u inter se congruant, primus vero cum secundo collatus dat $3ffh + 4ghh = hff + 2ghh$, seu $2ffh + 2ghh = 0$, ideoque $ff + gh = 0$: at secundus tertio aequatus dat $f^4 - ffgh - 2gghh = 0$, sive $(ff + gh)(ff - 2gh) = 0$, utrique ergo conditioni satisfit uno eodemque valore $h = -\frac{ff}{g}$.

11. Quoniam igitur invenimus $h = -\frac{ff}{g}$, reliqui valores sequenti modo exprimentur:

$$p = 2ff\zeta\zeta - 2fg\zeta\eta + gg\eta\eta$$
$$q = -\frac{ff}{g}\cdot\zeta\,(f\zeta - 2g\eta) = 2ff\zeta\eta - \frac{f^3}{g}\cdot\zeta\zeta,$$
$$r = -\frac{f^3}{g}\cdot\zeta\zeta - ff\zeta\eta + fg\eta\eta,$$
$$s = -ff\zeta\zeta - fg\zeta\eta + gg\eta\eta,$$

ubi notatu dignum evenit, ut in valoribus p et s producta $f\zeta$ et $g\eta$, tamquam simplices quantitates occurrant, quod quidem in litteris q et r non accidit. Verum quia totum negotium, tantum in ratione q ad r versatur, hi ambo valores multiplicentur per $-\frac{g}{f}$, ut sit $q = ff\zeta\zeta - 2fg\zeta\eta$ et $r = ff\zeta\zeta + fg\zeta\eta - gg\eta\eta$; hanc ob rem ut formulas nostras in compendium redigamus atque adeo ad duas quantitates revocemus, statuamus $f\zeta = m$ et $g\eta = n$, quo facto nostrae quatuor litterae ita se habebunt:

$$p = 2mm - 2mn + nn, \qquad q = mm - 2mn = m\,(m - 2n),$$
$$s = -mm - mn + nn, \qquad r = mm + mn - nn.$$

12. Quoniam vero res eodem redit sive quaepiam litera positive, sive negative accipiatur, ponamus

$$p = 2mm - 2mn + nn, \qquad q = mm - 2mn = m\,(m - 2n),$$
$$s = r = mm + mn - nn,$$

unde fit

$$p + s = 3mm - mn = m\,(3m - n),$$
$$p - s = mm - 3mn + 2nn = (m - n)\,(m - 2n),$$
$$q + r = 2mm - mn - nn = (m - n)\,(2m + n),$$
$$q - r = -3mn + nn = -n\,(3m - n).$$

Hic signum negationis in valore $q - r$ nihil plane turbat, tantum enim opus est litteras q et r inter se permutari, ita ut sit

$$p = 2mm - 2mn + nn, \quad q = mm + mn - nn,$$
$$s = mm + mn - nn, \quad r = mm - 2mn = m(m - 2n),$$

unde fit

$$p + s = 3mm - mn = m(3m - n),$$
$$p - s = mm - 3mn + 2nn = (m - n)(m - 2n),$$
$$q + r = 2mm - mn - nn = (2m + n)(m - n),$$
$$q - r = 3mn - nn = n(3m - n),$$

quibus valoribus in sequenti calculo utemur.

13. His constitutis valoribus, pro numeratore nostrae fractionis habebimus:

$$pp + ss = 5m^4 - 6m^3n + 7mmnn - 6mn^3 + 2n^4,$$

seu

$$pp + ss = (mm + nn)(5mm - 6mn + 2nn),$$

et

$$qq + rr = 2m^4 - 2m^3n + 3mmnn - 2mn^3 + n^4,$$

sive

$$qq + rr = (mm + nn)(2mm - 2mn + nn),$$

unde fractio nostra ad quadratum reducenda erit:

$$\frac{MM}{NN} = \frac{(5mm - 6mn + 2nn)(mm + nn)^2}{2n(2m + n)m^2(m - n)^2(m - 2n)^2(3m - n)^2(mm + mn + nn)^2}$$

hincque colligimus:

$$\frac{M}{N} = \frac{mm + nn}{m(m - n)(m - 2n)(3m - n)(mm + mn - nn)} \cdot \sqrt{\frac{5mm - 6mn + 2nn}{2n(2m + n)}};$$

totum ergo negotium huc est reductum, ut formula $\frac{5mm - 6mn + 2nn}{2n(2m + n)}$ quadratum efficiatur, id quod infinitis modis praestari posse manifestum est, statim atque unicus casus innotuerit.

14. Quo haec forma tractabilior reddatur, ponamus $2m - n = l$, ut sit $n = 2m - l$, et formula ad quadratum reducenda erit: $\frac{mm - 2ml + 2ll}{(4m - 2l)(4m - l)}$, ubi productum ex numeratore in denominatorem evolutum quippe quod etiam quadratum esse debet, perducit ad hanc conditionem

$$16m^4 - 44m^3l + 58mmll - 28ml^3 + 4l^4 = \Box,$$

cujus quum ambo termini extremi jam sint quadrati, per methodos satis cognitas facile est innumerabiles solutiones investigare; quem in finem ponamus $\frac{m}{l} = z$, ut habeamus hanc formulam

$$16z^4 - 44z^3 + 58zz - 28z + 4 = \Box;$$

quae ponendo $z = y - 2$; transit in hanc:

$$16y^4 - 172y^3 + 706yy - 1300y + 900 = \Box,$$

ubi iterum ambo extremi termini sunt quadrata.

15. Ad hoc negotium expediendum, praestabit resolutionem nostrae aequationis sive prioris, sive posterioris in genere docere. Sit igitur proposita haec aequatio generalis:

$$\alpha\alpha z^4 - 2\beta z^3 + \gamma zz - 2\delta z + \varepsilon\varepsilon = \Box;$$

atque pro idoneis valoribus ipsius z sequentes quatuor formulae per methodos consuetas reperiuntur:

$$\text{I.}\quad z=\frac{2\alpha(\beta\varepsilon-\alpha\delta)}{2\alpha^3\varepsilon+\beta\beta-\alpha\alpha\gamma},$$

$$\text{II.}\quad z=\frac{2\alpha\varepsilon^3+\delta\delta-\gamma\varepsilon\varepsilon}{2\varepsilon(\alpha\delta-\beta\varepsilon)},$$

$$\text{III.}\quad z=\frac{(2\alpha^3\varepsilon+\alpha\alpha\gamma-\beta\beta)(2\alpha^3\varepsilon-\alpha\alpha\gamma+\beta\beta)}{4\alpha\alpha(2\alpha^4\delta-\alpha\alpha\beta\gamma+\beta^3)},$$

$$\text{IV.}\quad z=\frac{4\varepsilon\varepsilon(2\beta\varepsilon^4-\gamma\delta\varepsilon\varepsilon+\delta^3)}{(2\alpha\varepsilon^3+\gamma\varepsilon\varepsilon-\delta\delta)(2\alpha\varepsilon^3-\gamma\varepsilon\varepsilon+\delta\delta)},$$

ubi quum litterae α et ε pro lubitu tam positive quam negative accipi queant, binae priores formulae geminos valores suppeditant.

16. Quemadmodum autem innumerabiles hujus aequationis solutiones inveniri oporteat, sequenti modo calculus instituatur. Sit f valor quicunque per praecedentes formulas inventus, ita ut nostra expressio

$$\alpha\alpha z^4-2\beta z^3+\gamma zz-2\delta z+\varepsilon\varepsilon,$$

posito $z=f$ fiat quadratum, sitque propterea

$$\alpha\alpha f^4-2\beta f^3+\gamma ff-2\delta f+\varepsilon\varepsilon=gg;$$

nunc igitur ponatur $z=x+f$ et nostra aequatio induet hanc formam:

$$\alpha\alpha x^4+\left.\begin{array}{l}4\alpha\alpha f\\-2\beta\end{array}\right\}x^3+\left.\begin{array}{l}6\alpha\alpha ff\\-6\beta f\\+\gamma\end{array}\right\}xx+\left.\begin{array}{l}4\alpha\alpha f^3\\-6\beta ff\\+2\gamma f\\-2\delta\end{array}\right\}x+gg=\square$$

quae aequatio brevitatis gratia ita repraesentetur:

$$aax^4-2bx^3+cxx-2dx+ee=\square$$

ita ut sit $aa=\alpha\alpha$, $b=\beta-2\alpha\alpha f$, $c=\gamma-6\beta f+6\alpha\alpha ff$, $d=\delta-\gamma f+3\beta ff-2\alpha\alpha f^3$, ac denique $ee=gg$, ubi sumi potest $a=\pm\alpha$ et $e=\pm g$. Tum vero quatuor novi valores pro z inveniuntur sequentes:

$$\text{I.}\quad z=f+\frac{2a(be-ad)}{2a^3e+bb-aac},$$

$$\text{II.}\quad z=f+\frac{2ae^3+dd-cee}{2e(ad-be)},$$

$$\text{III.}\quad z=f+\frac{(2a^3e+aac-bb)(2a^3e-aac+bb)}{4aa(2a^4d-aabc+b^3)},$$

$$\text{IV.}\quad z=f+\frac{4ee(2be^4-cdee+d^3)}{(2ae^3+cee-dd)(2ae^3-cee+dd)},$$

quoniam igitur quemcunque valorem pro z hoc modo inventum assumere licet, hinc numerus solutionum in infinitum augeri poterit.

17. Postquam autem pro z valor quicunque idoneus fuerit inventus, qui sit $z=\frac{h}{k}$, ob $z=\frac{m}{l}=\frac{m}{2m-n}$, habebimus $m=h$ et $n=2h-k$, ex quibus duobus numeris m et n reliquae quantitates sequenti modo determinantur:

$$p=2mm-2mn+nn,\quad q=mm+mn-nn,$$
$$s=mm+mn-nn,\qquad r=mm-2mn=m(m-2n),$$

ubi notasse juvabit esse:

$$pp + ss = (mm + nn)(5mm - 6mn + 2nn)$$

et

$$qq + rr = (mm + nn)(2mm - 2mn + nn) = (mm + nn)p,$$

atque hinc denique ambo nostri numeri quaesiti erunt

$$A = \frac{(mm+nn)^2(5mm-6mn+2nn)}{4m(m-2n)(mm+mn-nn)^2}$$

et

$$B = \frac{(mm+nn)^2(5mm-6mn+2nn)(2mm-2mn+nn)}{(3m-n)^2(m-n)^2mm(m-2n)(2m+n)}.$$

18. Ut autem etiam innotescat, quemadmodum hujusmodi valores inventi satisfaciant, ex binis numeris idoneis m et n prodeat formula radicalis

$$\sqrt{\frac{5mm-6mn+2nn}{2n(2m+n)}} = \frac{\mu}{\nu},$$

unde colligitur

$$\frac{M}{N} = \frac{(mm+nn)\mu}{\nu m(m-n)(m-2n)(3m-n)(mm+mn-nn)},$$

tum vero quoniam supra litteras q et r permutavimus, quaternae formulae propositae, sequenti modo ad quadrata reducentur

I. $\sqrt{(AB+A+B)} = \frac{M}{N}(pr+qs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)^2}{m(m-2n)(mm+mn-nn)},$

II. $\sqrt{(AB+A-B)} = \frac{M}{N}(pr-qs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)(m^4-8m^3n+6mmnn-n^4)}{m(m-n)(m-2n)(3m-n)(mm+mn-nn)},$

III. $\sqrt{(AB-A+B)} = \frac{M}{N}(pq+rs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)}{(m-n)(m-2n)},$

IV. $\sqrt{(AB-A-B)} = \frac{M}{N}(pq-rs) = \frac{\mu}{\nu}\cdot\frac{(mm+nn)}{m(3m-n)}.$

Aliae transformationes formulae resolvendae.

19. Quum tota quaestio huc sit perducta, ut ista formula (13)

$$\frac{5mm-6mn+2nn}{2n(2m+n)}, \quad \text{sive} \quad \frac{(2m-n)^2+(m-n)^2}{2n(2m+n)}$$

ad quadratum revocetur, ponamus $2m-n=t$ et $m-n=u$, ita ut sit $m=t-u$ et $n=t-2u$, hincque $2m+n=3t-4u$, atque nunc quadratum esse debeat

$$\frac{tt+uu}{(2t-4u)(3t-4u)} = \square, \quad \text{sive} \quad \frac{tt+uu}{(4u-2t)(4u-3t)} = \square$$

circa quam formulam observo, numeratorem cum denominatore alios factores communes habere non posse praeter 2 et 5. Hinc igitur sequitur numeratorem $tt+uu$ vel ipsum quadratum esse debere, vel duplum, vel quintuplum, vel decuplum quadratum. Unde quatuor casus resultant, quos singulos sequenti modo evolvamus.

20. Denotent litterae a et b binos cathetos trianguli rectanguli numerici, cujus hypotenusa sit $=c$, ita ut sit $aa+bb=cc$, nunc igitur pro primo casu faciamus $tt+uu=cc$, quod fit sumendo $t=a$ et $u=b$, atque hoc casu necesse est, ut fiat $(4b-2a)(4b-3a)=\square$.

Pro secundo casu faciamus $tt+uu=2cc$, quod fit sumendo $t=a-b$ et $u=a+b$, atque nunc necesse est ut sit $(a+3b)(a+7b)=\square$.

Pro tertio casu faciamus $tt + uu = 5cc$, quod fit sumendo $t = a + 2b$ et $u = 2a - b$; tum enim ob $4u - 2t = 4a - 8b$ et $4u - 3t = 5a - 10b$, formula ad quadratum reducenda erit $(6a - 8b)(a - 2b) = \square$, hoc est $(4b - 2a)(4b - 3a) = \square$, quae cum casu primo perfecte congruit.

Pro casu denique quarto, faciamus $tt + uu = 10cc$, quod fit sumendo $t = 3a + b$ et $u = a - 3b$, tum enim ob $4u - 2t = -14b - 2a$ et $4u - 3t = -5a - 15b$, formula ad quadratum reducenda erit $(3b + a)(7b + a) = \square$, prorsus uti in casu secundo. Verum hic notandum est, casum tertium et quartum adhuc alio modo expediri posse. Si enim pro tertio ponamus $t = a + 2b$ et $u = b - 2a$, ob $4u - 2t = -10a$ et $4u - 3t = -2b - 11a$, formula ad quadratum reducenda erit $2a(11a + 2b) = \square$.

Pro casu quarto autem, si ponamus $t = 3a + b$ et $u = 3b - a$, ob $4u - 2t = 10b - 10a$ et $4u - 3t = 9b - 13a$, formula ad quadratum reducenda est $(a - b)(13a - 9b) = \square$. Verum plerumque quoties his duobus casibus satisfieri potest, toties numeri t et u communi factore 5 praediti reperiuntur, ideoque ad novas solutiones non perducunt.

21. His igitur duobus casibus postremis relictis, circa quatuor praecedentes omnino memoratu dignum est, quod primus et tertius, tum vero etiam secundus et quartus ad eandem formulam perduxerit, quare pro primo et tertio, si numeri a et b ita fuerint comparati, ut formula

$$(4b - 2a)(4b - 3a)$$

fiat quadratum, tum duplici modo inde idonei valores pro t et u obtinentur; priori enim modo habebimus $t = a$ et $u = b$, altero vero modo $t = a + 2b$ et $u = 2a - b$. Simili modo pro casibus secundo et quarto, si fuerit formula $(3b + a)(7b + a)$ quadratum, tum etiam duo casus oriuntur, alter $t = a - b$ et $u = a + b$, alter vero $t = 3a + b$ et $u = a - 3b$. Operae igitur pretium erit has geminas resolutiones accuratius exponere.

I. *Si fuerit* $(4b - 2a)(4b - 3a) = \square$, *existente* $aa + bb = cc$.

22. Hinc igitur primo statim deducimus fractionem supra (18) introductam $\frac{\mu}{\nu} = \frac{cc}{(4b-2a)(4b-3a)}$; deinde pro priori resolutione habebimus

$$\begin{array}{ll} t = a, & m = a - b, \\ u = b, & n = a - 2b, \\ p = aa - 2ab + 2bb, & r = (a - b)(3b - a), \\ q = aa - ab - bb, & s = aa - ab - bb, \\ \frac{p}{s} = \frac{aa - 2ab + 2bb}{aa - ab - bb}, & \frac{q}{r} = \frac{aa - ab - bb}{(a-b)(3b-a)}, \end{array}$$

$$mm + nn = 2aa - 6ab - 5bb;$$

pro altera vero solutione

$$\begin{array}{ll} t = a + 2b, & m = 3b - a, \\ u = 2a - b, & n = 4b - 3a, \\ p = 5(aa - 2ab + 2bb), & r = -5(a - b)(3b - a), \\ q = -5(aa - ab - bb), & s = -5(aa - ab - bb), \\ \frac{p}{s} = \frac{aa - 2ab + 2bb}{aa - ab - bb}, & \frac{q}{r} = \frac{aa - ab - bb}{(a-b)(3b-a)}, \end{array}$$

unde manifestum est has duas solutiones a se invicem non differre.

23. Speciales autem solutiones, quae ex hac formula primo intuitu derivantur, sunt sequentes

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
0	1	-1	-2	$\frac{2}{1}$	$\frac{1}{3}$
4	3	1	-2	$\frac{2}{1}$	$\frac{1}{1}$
12	5	7	2	$\frac{74}{59}$	$\frac{59}{21}$

quarum binae priores scopo nostro non conveniunt, tertia vero idoneam praebet solutionem, atque adeo ab illa, quam olim jam inveni, diversam; quum enim sit $pp + ss = 8957 = 53.169$ et $qq + rr = 3922 = 53.74$, erunt ambo quaesiti numeri

$$A = \frac{169.53^2.74}{4.74.59^2.21} = \frac{169.53^2}{4.21.59^2},$$

$$B = \frac{169.74.53^2}{2.16.3.5^2.7.19^2} = \frac{169.37.53^2}{16.3.5^2.7.19^2}.$$

24. Consideremus autem attentius hanc formulam: $(4b - 2a)(4b - 3a) = \square$, et quia numeri a et b sunt catheti trianguli rectanguli, atque evidens est, pro a sumi debere numerum parem, pro b vero imparem, statuamus $a = 2de$ et $b = dd - ee$, ut sit hypotenusa $c = dd + ee$, tum vero erit

$$4b - 2a = 4(dd - de - ee) \quad \text{et} \quad 4b - 3a = 4dd - 6de - 4ee,$$

quorum productum quum quadratum esse debeat, necesse est, ut utriusque quadrans fiat quadratum, hoc est

$$\text{I.} \quad dd - de - ee = \square,$$

$$\text{II.} \quad dd - \tfrac{3}{2}de - ee = \square,$$

ubi quum numerorum d et e alter debeat esse par, alter impar, etiam posterior numeris integris constat. Quod autem ad priorem attinet, quum sit $dd - de - ee = (d - \frac{1}{2}e)^2 - 5\frac{e^2}{4}$, ponamus $d - \frac{1}{2}e = rr + 5ss$ et $\frac{1}{2}e = 2rs$, tum enim fiet $dd - de - ee = (rr - 5ss)^2$; at vero habebimus $e = 4rs$ et $d = rr + 2rs + 5ss$, hincque $dd - ee = r^4 + 4r^3s - 2rrss + 20rs^3 + 25s^4$ et $de = 4r^3s + 8rrss + 20rs^3$, unde altera conditio postulat: $r^4 - 2r^3s - 14rrss - 10rs^3 + 25s^4 = \square$.

25. Statuamus hic $\frac{r}{s} = z$, ut habeamus hanc formulam $z^4 - 2z^3 - 14zz - 10z + 25 = \square$, quae cum formula supra data (15) comparata praebet: $\alpha = \pm 1$, $\beta = 1$, $\gamma = -14$, $\delta = 5$, $\varepsilon = \pm 5$, unde pro z quatuor sequentes expressiones elicimus:

$$\text{I.} \quad z = \frac{2\alpha(\varepsilon - 5\alpha)}{2\alpha^3\varepsilon + 15} = \frac{2(\alpha\varepsilon - 5)}{2\alpha\varepsilon + 15}$$

hinc vel $z = 0$, vel $z = -4$;

$$\text{II.} \quad z = \frac{50\alpha\varepsilon + 375}{2(5\alpha\varepsilon - 25)} = \frac{10\alpha\varepsilon - 75}{2(\alpha\varepsilon - 5)}$$

vel $z = \infty$, vel $z = -\frac{5}{4}$;

$$\text{III.} \quad z = \frac{(2\alpha\varepsilon - 14 - 1)(2\alpha\varepsilon + 14 + 1)}{4(10 + 14 + 1)} = -\frac{125}{100} = -\frac{5}{4}.$$

$$\text{IV.}\quad z = \frac{100(1250 + 70.25 + 5.25)}{(50\alpha - 15.25)(50\alpha + 15.25)} = \frac{4.25^2.125}{25^2(2\alpha + 15)(2\alpha - 15)} = -4.$$

Ex valore $z = -4$ oriuntur valores $r = 4$, $s = -1$, $d = 13$, $e = -16$, hincque $a = 416$ et $b = 87$, unde oritur $\frac{p}{s} = \frac{23362}{25859}$ et $\frac{q}{r} = \frac{25859}{10199}$; at ex valore $z = -\frac{5}{4}$ habemus $r = 5$, $s = -4$, $d = 65$, $e = -80$, qui per quinarium ad terminos minores reducti praebent ut ante, $d = 13$ et $e = -16$, ubi notasse juvabit ex his valoribus a et b praegrandes numeros pro p, q, r, s esse prodituros.

26. At circa binas illas formulas notasse juvabit, utramque etiam quadrato negativo aequari posse, verum tum solutio eadem exsurgit, nisi quod valores pro a et b fiant negativi. Ceterum hic notari convenit, ultimae aequationi etiam valorem $z = -3$ satisfacere, etiamsi eum non per methodum consuetam detexerimus, inde autem fit $r = 3$ et $s = -1$; hincque porro $d = 2$ et $e = -3$; unde fit $a = -12$ et $b = -5$, quem casum jam supra evolvimus.

II. *Si fuerit* $(3b + a)(7b + a) = \square$.

27. Hic statim apparet sumi debere $a = dd - ee$ et $b = 2de$, ut fiat $c = dd + ee$, tum ergo sequentes duae formulae quadrata esse debent

$$dd + 6de - ee = \square \quad \text{et} \quad dd + 14de - ee = \square.$$

Quum prior sit $= (d + 3e)^2 - 10ee$, si ponamus $\zeta\eta = 10$, ac statuamus $d + 3e = \zeta rr + \eta ss$ et $e = 2rs$, fiet illa formula $= (\zeta rr - \eta ss)^2$, tum autem erit $d = \zeta rr - 6rs + \eta ss$ et $e = 2rs$; hinc ergo pro altera formula, quae est $(d + 7e)^2 - 50ee$, erit $d + 7e = \zeta rr + 8rs + \eta ss$, ideoque haec formula abit in $\zeta\zeta r^4 + 16\zeta r^3 s - 116rrss + 16\eta rs^3 + \eta\eta s^4 = \square$, unde per methodum supra indicatam infinitae solutiones inveniri possunt; ubi notasse juvabit esse vel $\zeta = 1$ et $\eta = 10$, vel $\zeta = 2$ et $\eta = 5$.

28. Quum autem idonei valores pro a et b fuerint inventi, duplici modo inde litterae t et u definiri poterunt. Priore modo fit $t = a - b$ et $u = a + b$, hinc $m = t - u = -2b$ et $n = -a - 3b$, ideoque

$$p = mm + (m - n)^2 = aa + 2ab + 5bb,$$

$$q = s = mm + n(m - n) = -aa - 4ab + bb$$

$$\text{et} \quad r = m(m - 2n) = -4b(a + 2b),$$

ita ut sit

$$\frac{p}{s} = \frac{aa + 2ab + 5bb}{aa + 4ab - bb} \quad \text{et} \quad \frac{q}{r} = \frac{aa + 4ab - bb}{4b(a + 2b)}.$$

Posteriore vero modo fit $t = 3a + b$ et $u = a - 3b$, unde $m = 2a + 4b$ et $n = a + 7b$, hincque porro ob $m - n = a - 3b$, fit

$$p = 5(aa + 2ab + 5bb), \quad q = s = 5(aa + 4ab - bb) \quad \text{et} \quad r = 5.4b(a + 2b)$$

sicque patet hunc posteriorem casum ad priorem redire.

29. Simpliciores autem solutiones, quas facili negotio divinando elicere licet, sunt sequentes:

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
1	0	-0	-1	$\frac{1}{1}$	$\frac{1}{0}$
-3	4	-8	-9	$\frac{13}{11}$	$\frac{11}{16}$
-35	12	-24	-1	$\frac{1105}{599}$	$\frac{599}{528}$

Hic secundus casus praebet illam ipsam solutionem, quam jam olim dederam. His autem duabus formulis pertractatis adjungamus insuper binas postremas supra (20) inventas.

III. *Si fuerit* $2a(11a+2b)=\square$.

30. Casus simpliciores, qui statim se offerunt, sunt:

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
0	1	1, 1	0, 0	$\frac{2}{1}$	$\frac{1}{1}$
4	3	15, 3	20, 4	$\frac{2}{1}$	$\frac{1}{3}$
16	-63	-15, -3	80, 16	$\frac{74}{59}$	$\frac{59}{21}$

ubi ex datis a et b fit $t=a+2b$ et $u=b-2a$, hincque, ut ante, $m=t-u=3a+b$ et $n=t-2u=5a$. Hae solutiones autem jam in superioribus continentur.

IV. *Si fuerit* $(a-b)(13a-9b)=\square$.

31. Inventis idoneis valoribus pro a et b, erit $t=3a+b$ et $u=3b-a$, hinc

$$m=4a-2b=2(2a-b) \quad \text{et} \quad n=5(a-b),$$

atque ob $m-n=3b-a$, atque $m-2n=2(4b-3a)$ habebimus

$$\frac{p}{s}=\frac{17aa-22ab+13bb}{11aa+4ab-11bb} \quad \text{et} \quad \frac{q}{r}=\frac{11aa+4ab-11bb}{4(6aa-11ab+4bb)}.$$

Solutiones autem simpliciores hinc oriundae sunt

a	b	m	n	$\frac{p}{s}$	$\frac{q}{r}$
0	1	-2	-5	$\frac{13}{11}$	$\frac{11}{16}$
4	$+3$	10, 2	5, 1	$\frac{1}{1}$	$\frac{1}{0}$

ubi memoratu dignum evenit, quod statim primum tentamen quo $a=0$ et $b=1$, praebeat solutionem jam dudum inventam.

32. Quod si pro ulteriore hujus formulae evolutione ponamus $a=2de$ et $b=dd-ee$, fiet $a-b=ee+2de-dd$, sive mutandis signis, ut $(b-a)(9b-13a)=\square$, erit

$$b-a=dd-2de-ee \quad \text{et} \quad 9b-13a=9dd-26de-9ee,$$

reddamus nunc priorem quadratum, quae cum sit $(d-e)^2-2ee$, statuamus $d-e=rr+2ss$ et $e=2rs$, tum enim fiet $dd-2de-ee=(rr-2ss)^2$, tum vero alter factor ob

$$dd-ee=r^4+4r^3s+4rrss+8rs^3+4s^4,$$

erit
$$9r^4-16r^3s-68rrss-32rs^3+36s^4,$$

ubi casus primo intuitu se offerentes sunt: 1) $r=1$, $s=0$; 2) $r=0$, $s=1$; 3) $r=1$ et $s=-1$; 4) $r=2$ et $s=-1$; 5) $r=1$ et $s=2$.

33. Pro horum casuum primo habemus $d=1$ et $e=0$; hinc $a=0$ et $b=1$, qui jam occurrit; pro secundo habemus $d=2$ et $e=0$, hinc $a=0$ et $b=1$, qui a praecedente non differt. At pro tertio habemus $d=1$ et $e=-2$, hinc $a=-4$ et $b=-3$, qui supra jam est tractatus; pro quarto habemus $d=2$ et $e=-4$, sive $d=1$ et $e=-2$, unde fit $a=-4$ et $b=-3$, ut praecedens; pro quinto denique habemus $d=13$ et $e=4$, hinc $a=104$ et $b=153$, ex quibus numeri praegrandes pro quaesitis A et B resultant, quibus non immoramur.

34. Imprimis autem quoque notatu dignus est casus, quo invenimus $\frac{p}{s}=\frac{2}{1}$ et $\frac{q}{r}=\frac{1}{3}$, sive $\frac{q}{r}=\frac{3}{1}$, unde deducuntur numeri quaesiti $A=\frac{25}{12}$ et $B=\frac{25}{12}$, ita ut ambo numeri quaesiti hoc casu fiant aequales, quod quidem scopo problematis minus convenit. Si enim numeri aequales desiderentur, ob eorum differentiam evanescentem quaestio huc rediret, ut inveniatur numerus A, ita ut tam $AA+2A$, quam $AA-2A$ fiat quadratum, quod quidem est facillimum, statuatur enim

$$AA=\frac{aa+bb}{nn} \quad \text{et} \quad 2A=\frac{2ab}{nn},$$

fiet utique

$$\sqrt{(AA+2A)}=\frac{a+b}{n} \quad \text{et} \quad \sqrt{(AA-2A)}=\frac{a-b}{n};$$

verum nunc requiritur ut $aa+bb$ sit quadratum, quem in finem ponamus $a=pp-qq$ et $b=2pq$, ut fiat $A=\frac{pp+qq}{n}$; est vero etiam $A=\frac{2pq(pp-qq)}{nn}$, unde fit $n(pp+qq)=2pq(pp-qq)$ et $n=\frac{2pq(pp-qq)}{pp+qq}$, ita ut numerus quaesitus in genere sit $A=\frac{(pp+qq)^2}{2pq(pp-qq)}$, tales ergo numeri sunt sequentes:

$$1)\ A=\frac{25}{12}, \quad 2)\ A=\frac{169}{60}, \quad 3)\ A=\frac{289}{120}, \quad 4)\ A=\frac{625}{168} \text{ etc.}$$

35. Pro solutionibus autem ad quaestionem propositam accommodatis, duae in numeris non nimis magnis notatu dignae videntur, quarum prior est ea ipsa, quam jam dudum inveni, qua erat

$$A=\frac{13.29^2}{8.9^2} \quad \text{et} \quad B=\frac{5.29^2}{32.11^2}, \quad \text{sive} \quad A=\frac{10933}{648} \quad \text{et} \quad B=\frac{4205}{3872},$$

unde

$$\sqrt{(AB+A+B)}=\frac{7.29.37}{16.9.11}$$
$$\sqrt{(AB+A-B)}=\frac{29^2}{16.3.11}$$
$$\sqrt{(AB-A+B)}=\frac{29^2}{16.9}$$
$$\sqrt{(AB-A-B)}=\frac{29}{48}.$$

Pro altera vero solutione orta ex valoribus:

$$\frac{p}{s}=\frac{74}{59} \quad \text{et} \quad \frac{q}{r}=\frac{59}{21}$$

obtinemus:

$$A=\frac{13^2.53^2}{4.21.59^2} \quad \text{et} \quad B=\frac{13^2.37.53^2}{16.3.5^2.7.19^2}$$

unde

$$\sqrt{(AB+A+B)}=\frac{13.53}{8.3.7}$$

$$\sqrt{(AB+A-B)}=\frac{13.53^2}{8.3.5.7.19}$$

$$\sqrt{(AB-A+B)}=\frac{13.53^2}{8.3.7.59}$$

$$\sqrt{(AB-A-B)}=\frac{13.41.47.53}{8.3.5.7.19.59}.$$



XXX.

Problema algebraicum ob affectiones prorsus singulares memorabile.

(N. Comment. XV. 1770. p. 75. Exhib. 1770 Mart. 5.)

Problema, cujus affectiones hic contemplandas suscipio, ita se habet:

Invenire novem numeros ita in quadratum disponendos:

$$\begin{matrix} A, & B, & C, \\ D, & E, & F, \\ G, & H, & J, \end{matrix}$$

ut satisfiat duodecim sequentibus conditionibus:

$$\begin{array}{llll} 1) & AA + DD + GG = 1, & 4) & AB + DE + GH = 0 \\ 2) & BB + EE + HH = 1, & 5) & AC + DF + GJ = 0 \\ 3) & CC + FF + JJ = 1, & 6) & BC + EF + HJ = 0 \\ 7) & AA + BB + CC = 1, & 10) & AD + BE + CF = 0 \\ 8) & DD + EE + FF = 1, & 11) & AG + BH + CJ = 0 \\ 9) & GG + HH + JJ = 1, & 12) & DG + EH + FJ = 0. \end{array}$$

Circa hoc problema sequentia observo.

I. Cum numerus conditionum implendarum superet numerum quantitatum determinandarum, problema hoc plus quam determinatum videtur. Utcunque enim conditiones praescriptae perpendantur, nulla alia relatio, qua aliquae in reliquis jam contineantur, in iis deprehenditur, nisi quod summa conditionum 7), 8), 9) conveniat cum summa conditionum 1), 2), 3); unde unica harum duodecim conditionum in reliquis jam contineri videtur; qua remota tamen adhuc undecim conditiones relinquuntur, quae binario numerum quantitatum incognitarum excedunt. Hic equidem tantum de ejusmodi relatione loquor, quae has conditiones consideranti occurrit, revera enim aliquot necessariae relationes inter eas intercedunt, quae autem vix ante animadvertuntur, quam problema perfecte fuerit solutum.

II. Deinde observo hoc problema non solum non esse plus quam determinatum, sed adeo esse indeterminatum, ita ut novem numerorum quaesitorum tres pro lubitu accipere liceat, nihiloque minus omnibus conditionibus praescriptis satisfieri queat. Dummodo enim sex prioribus conditionibus fuerit satisfactum, reliquae sex sponte implentur, atque omnino fieri non potest, ut sex prioribus satisfiat quin simul omnibus satisfiat. Quocirca problema propositum ejusdem prorsus indolis maneret, etiamsi sex posteriores conditiones plane omitterentur; ac tum ei insigne theorema istud adjungi posset.

Quodsi novem numeri A, B, C, D, E, F, G, H, J, *ita fuerint comparati, ut* 6 *prioribus conditionibus satisfaciant, tum etiam necessario sex posterioribus satisfacient.*

Quod theorema pro difficillimo demonstratu venditare non dubito, neque video quomodo demonstratio adornari queat, nisi solutio problematis fuerit explorata.

III. Neque vero hoc problema pro otiosa speculatione seu mero lusu ingenii est habendum, sed potius in doctrina de superficierum natura est maximi momenti. Cum enim natura superficiei per aequationem inter ternas coordinatas tribus axibus inter se normalibus parallelas exprimi soleat, talis aequatio mutandis axibus in infinitum variari potest, etiamsi axium communis intersectio in eodem puncto statuatur. Quoniam igitur eadem superficies infinitis aequationibus diversis inter ternas coordinatas definiri potest, plurimum interest earum characterem communem nosse, qui in eo consistit, ut si coordinatae ternis quibusdam axibus datis parallelae sint x, y, z; quae autem aliis quibuscunque axibus constituuntur parallelae, fuerint X, Y, Z, eorum relatio mutua semper hujusmodi formulis contineatur:

$$X = Ax + By + Cz, \quad Y = Dx + Ey + Fz, \quad Z = Gx + Hy + Jz,$$

qui novem coefficientes ita comparati sint necesse est, ut inde fiat:

$$XX + YY + ZZ = xx + yy + zz,$$

quandoquidem his formulis quadratum intervalli, quo superficiei punctum ab initio coordinatarum distat, exprimitur. Quod fieri nequit, nisi hae sex aequationes habeant locum:

$$AA + DD + GG = 1, \quad BB + EE + HH = 1, \quad CC + FF + JJ = 1,$$
$$AB + DE + GH = 0, \quad AC + DF + GJ = 0, \quad BC + EF + HJ = 0,$$

quae sunt ipsae sex priores conditiones nostri problematis.

IV. Quocunque autem modo hoc problema secundum algebrae praecepta tentetur, ob tantum incognitarum numerum semper ad calculos vehementer intricatos pervenitur, ex quibus neutiquam solutionem commodam expectare liceat. Theoriam quidem angulorum in subsidium vocando, haud difficulter solutio satis concinna obtinetur, verum haec methodus vix ad alias hujus generis quaestiones magis complicatas traduci poterit: veluti si circa 16, 25, 36, etc. numeros, pariter in quadratum disponendos similis quaestio instituatur, ut summa quadratorum, per singulas columnas tam verticales quam horizontales sumtorum, unitati aequetur, simul vero summae productorum secundum binas columnas itidem tam verticales quam horizontales ad nihilum redigantur. Methodum ergo etiam ad has quaestiones patentem, quae utique in analysi maximi momenti est putanda, deinceps sum expositurus, postquam demonstrationem theorematis § II memorati, atque solutionem problematis initio propositi ope sinuum et cosinuum tradidero.

Demonstratio theorematis § II propositi.

V. Assumo ergo novem numeros nostros A, B, C, D, E, F, G, H, J, ita esse comparatos ut sit

$$1)\ AA + DD + GG = 1, \qquad 4)\ AB + DE + GH = 0,$$
$$2)\ BB + EE + HH = 1, \qquad 5)\ AC + DF + GJ = 0,$$
$$3)\ CC + FF + JJ = 1, \qquad 6)\ BC + EF + HJ = 0,$$

quarum tres posteriores ita repraesento:

4) $AB = -DE - GH$, 5) $AC = -DF - GJ$, 6) $BC = -EF - HJ$,

unde concludo fore:

$$\frac{4).5)}{6)} \ldots \frac{AABC}{BC} = AA = -\frac{(DE+GH)(DF+GJ)}{EF+HJ}$$

qui valor ipsius AA in prima aequatione positus dat:

$$-(DE+GH)(DF+GJ)+(EF+HJ)(DD+GG) = EF+HJ$$

factaque evolutione:

$$-DEGJ - DFGH + DDHJ + EFGG = EF + HJ,$$

cujus aequationis primum membrum manifesto in hos factores resolvitur:

$$(DH-EG)(DJ-FG) = EF+HJ.$$

VI. Cum igitur sit $EF + HJ = -BC$, erit

$$BC = (EG-DH)(DJ-FG)$$

similique modo colligetur fore

$$AC = (FH-EJ)(EG-DH) \quad \text{et} \quad AB = (DJ-FG)(FH-EJ),$$

quarum duarum posteriorum productum, per primam divisum, praebet

$$AA = (FH-EJ)^2 \quad \text{hincque} \quad A = \pm(FH-EJ);$$

quia autem singulos numeros tam negative quam positive capere licet, ambiguitas signi nullam variationem inferre est censenda, unde sumto superiori habebimus:

$$A = FH - EJ, \quad B = DJ - FG, \quad C = EG - DH.$$

Cum autem ex rei natura columnas verticales inter se permutare liceat, hinc per analogiam concludimus fore

$$D = BJ - CH, \quad E = CG - AJ, \quad F = AH - BG$$
$$G = CE - BF, \quad H = AF - CD, \quad J = BD - AE.$$

VII. En ergo novem novas determinationes, quae in sex conditionibus praescriptis necessario involvuntur, et quas insuper ad 12 conditiones initio propositas adjicere potuissemus. Verum hae ipsae novem determinationes, quas sequenti modo indicabo:

13) $A = FH - EJ$, 16) $D = BJ - CH$, 19) $G = CE - BF$,

14) $B = DJ - FG$, 17) $E = CG - AJ$, 20) $H = AF - CD$,

15) $C = EG - DH$, 18) $F = AH - BG$, 21) $J = BD - AE$,

facile ad conditiones sex posteriores, initio propositas deducunt. Nam formulae 13) per D, 14) per E et 15) per F multiplicatae et in unam summam collectae dant:

$$AD + BE + CF = + DFH + DEJ + EFG - DEJ - EFG - DFH = 0,$$

quae est ipsa conditio 10) initio proposita, similique modo $13).G + 14).H + 15).J$ dabit conditionem 11), et $16).G + 17).H + 18).J$ conditionem 12), ita ut sit:

10) $AD + BE + CF = 0$, 11) $AG + BH + CJ = 0$, 12) $DG + EH + FJ = 0$.

VIII. Denique si in formula 13) valores literarum E et F ex formulis 17) et 18) substituantur, emergit haec aequatio:

$$A = AHH - BGH - CGJ + AJJ = A(HH+JJ) - G(BH+CJ)$$

at ex aequatione 11) est $BH + CJ = -AG$, unde colligitur:

$$A = A(GG + HH + JJ), \quad \text{ideoque vel} \quad A = 0, \quad \text{vel} \quad GG + HH + JJ = 1.$$

Cum autem simili modo ex formulis 14), 15), 16), 17) et 18) eliciantur aequationes:

$$B = B(GG + HH + JJ), \qquad C = C(GG + HH + JJ), \qquad D = D(GG + HH + JJ),$$
$$E = E(GG + HH + JJ) \quad \text{et} \quad F = F(GG + HH + JJ)$$

neque litterae A, B, C, D, E, F omnes simul evanescant, necesse est sit $GG + HH + JJ = 1$, quae est conditio 9) hocque modo ostenditur esse:

$$7) \quad AA + BB + CC = 1, \qquad 8) \quad DD + EE + FF = 1, \qquad 9) \quad GG + HH + JJ = 1,$$

quae est demonstratio completa theorematis propositi.

Solutio problematis initio propositi.

IX. Statuamus $A = \cos\zeta$, et cum conditiones 1) et 7) praebeant:

$$DD + GG = \sin^2\zeta \quad \text{et} \quad BB + CC = \sin^2\zeta$$

his in genere satisfaciemus ponendo:

$$B = \sin\zeta\cos\eta; \quad C = \sin\zeta\sin\eta, \quad D = \sin\zeta\cos\vartheta, \quad G = \sin\zeta\sin\vartheta.$$

Considerentur jam conditiones 17) et 21), quae factis his substitutionibus induent has formas:

$$17) \quad E = \sin^2\zeta\sin\eta\sin\vartheta - J\cos\zeta, \quad \text{seu} \quad E + J\cos\zeta = \sin^2\zeta\sin\eta\sin\vartheta,$$
$$21) \quad J = \sin^2\zeta\cos\eta\cos\vartheta - E\cos\zeta, \quad \text{seu} \quad J + E\cos\zeta = \sin^2\zeta\cos\eta\cos\vartheta,$$

Hinc 17) — 21).cos ζ et 21) — 17).cos ζ dant:

$$E(1 - \cos^2\zeta) = \sin^2\zeta(\sin\eta\sin\vartheta - \cos\zeta\cos\eta\cos\vartheta),$$
$$J(1 - \cos^2\zeta) = \sin^2\zeta(\cos\eta\cos\vartheta - \cos\zeta\sin\eta\sin\vartheta),$$

unde colligitur:

$$E = \sin\eta\sin\vartheta - \cos\zeta\cos\eta\cos\vartheta \quad \text{et} \quad J = \cos\eta\cos\vartheta - \cos\zeta\sin\eta\sin\vartheta.$$

X. Simili modo conditiones 18) et 20) modo ante demonstratae, factis substitutionibus suppeditant has aequationes:

$$18) \quad F = H\cos\zeta - \sin^2\zeta\cos\eta\sin\vartheta, \quad \text{seu} \quad F - H\cos\zeta = -\sin^2\zeta\cos\eta\sin\vartheta$$
$$20) \quad H = F\cos\zeta - \sin^2\zeta\sin\eta\cos\vartheta, \quad \text{seu} \quad H - F\cos\zeta = -\sin^2\zeta\sin\eta\cos\vartheta$$

unde formae 18) + 20).cos ζ et 20) + 18).cos ζ producunt

$$F(1 - \cos^2\zeta) = -\sin^2\zeta(\cos\eta\sin\vartheta + \cos\zeta\sin\eta\cos\vartheta),$$
$$H(1 - \cos^2\zeta) = -\sin^2\zeta(\sin\eta\cos\vartheta + \cos\zeta\cos\eta\sin\vartheta),$$

unde ob $1 - \cos^2\zeta = \sin^2\zeta$ elicitur

$$F = -\cos\eta\sin\vartheta - \cos\zeta\sin\eta\cos\vartheta \quad \text{et} \quad H = -\sin\eta\cos\vartheta - \cos\zeta\cos\eta\sin\vartheta$$

sicque novem numeri conditionibus praescriptis satisfacientes ita sunt definiti, ut tres anguli ζ, η, ϑ arbitrio nostro relinquantur, in quo criterium solutionis completae cernitur.

XI. Solutio ergo completa nostri problematis ita se habet, ut novem numeri quaesiti sequentes sortiantur valores:

$A = \cos\zeta$	$B = \quad \sin\zeta\cos\eta$	$C = \quad \sin\zeta\sin\eta$
$D = \sin\zeta\cos\vartheta$	$E = \quad \sin\eta\sin\vartheta - \cos\zeta\cos\eta\cos\vartheta$	$F = -\cos\eta\sin\vartheta - \cos\zeta\sin\eta\cos\vartheta$
$G = \sin\zeta\sin\vartheta$	$H = -\sin\eta\cos\vartheta - \cos\zeta\cos\eta\sin\vartheta$	$J = +\cos\eta\cos\vartheta - \cos\zeta\sin\eta\sin\vartheta$

quibus valoribus non solum sex conditiones priores, quibus problema determinatur, sed etiam sex posteriores, atque adeo etiam novem novae § VII exhibitae, adimplentur. Haecque solutio istum praestat usum, ut inde facili negotio solutiones in numeris rationalibus, quotcunque libuerit, reperire liceat, tres scilicet angulos ζ, η, ϑ, ita capi opus est, ut eorum tam sinus quam cosinus rationaliter exprimantur. Hinc solutio satis simplex prodibit sumendo

$$\cos\zeta = \tfrac{3}{5}, \quad \sin\zeta = \tfrac{4}{5}, \quad \cos\eta = \tfrac{3}{5}, \quad \sin\eta = \tfrac{4}{5}, \quad \cos\vartheta = \tfrac{5}{13}, \quad \sin\vartheta = \tfrac{12}{13}.$$

Methodus generalis hujusmodi problemata resolvendi.

XII. Methodus generalis, quam hic sum traditurus, ex principio supra § III memorato est petita, ubi ostendi problema propositum eo redire, ut ex ternis variabilibus x, y, z, aliae tres X, Y, Z, per hujusmodi formulas $\alpha x + \beta y + \gamma z$ ita determinentur, ut fiat

$$X^2 + Y^2 + Z^2 = x^2 + y^2 + z^2,$$

haecque determinatio maxime sit generalis; tum enim coefficientes trium harum formularum $\alpha x + \beta y + \gamma z$ pro novis variabilibus X, Y, Z resultantium, erunt ipsi illi novem numeri, qui in problemate desiderantur. Hic igitur duae conditiones probe sunt perpendendae, quarum altera est, ut valores ipsarum X, Y, Z simpliciter per hujusmodi formulas $\alpha x + \beta y + \gamma z$ exprimantur, altera vero, ut tum fiat $X^2 + Y^2 + Z^2 = x^2 + y^2 + z^2$. Nisi enim illa conditio adesset, quaestio foret per methodum Diophanteam solutu facilis, dum tantum trium quadratorum summa in tria alia quadrata resolvi deberet, id quod nihil habet difficultatis.

XIII. Quoniam vero rem eo deducere animus est, ut methodus ad quaestiones continuo magis complicatas extendi queat, a casu simplicissimo exordiar, quo propositis tantum duabus variabilibus x et y, ex iis aliae duae X et Y per hujusmodi formulas $\alpha x + \beta y$ definiri debeant, ut fiat $X^2 + Y^2 = x^2 + y^2$. Hunc in finem posito

$$X = \alpha x + \beta y \quad \text{et} \quad Y = \gamma x + \delta y$$

necesse est fiat:

$$\alpha\alpha + \gamma\gamma = 1, \quad \beta\beta + \delta\delta = 1, \quad \alpha\beta + \gamma\delta = 0.$$

Statuamus ergo $\alpha = \cos\zeta$ et $\beta = \cos\eta$, ut habeatur $\gamma = \sin\zeta$ et $\delta = \sin\eta$, sicque duabus prioribus conditionibus satisfiat: tum vero tertia dabit $\cos\zeta\cos\eta + \sin\zeta\sin\eta = \cos(\zeta - \eta) = 0$, ex quo erit $\zeta - \eta = 90^\circ$, ideoque $\eta = \zeta - 90^\circ$, ac propterea $\cos\eta = \sin\zeta$ et $\sin\eta = -\cos\zeta$. Unde patet si capiatur:

$$X = x\cos\zeta + y\sin\zeta \quad \text{et} \quad Y = x\sin\zeta - y\cos\zeta$$

fore $X^2 + Y^2 = x^2 + y^2$.

XIV. Hoc lemmate praemisso, ex propositis tribus variabilibus x, y, z primo alias tres x', y', z' ita definio, ut sit

$$x' = x\cos\zeta + y\sin\zeta, \quad y' = x\sin\zeta - y\cos\zeta \quad \text{et} \quad z' = z;$$

hoc enim modo certo erit

$$x'x' + y'y' + z'z' = xx + yy + zz.$$

Deinde ex his simili modo alias tres x'', y'', z'' deduco, ut sit

$$x'' = x', \quad y'' = y'\cos\eta + z'\sin\eta, \quad z'' = y'\sin\eta - z'\cos\eta$$

atque hinc tandem quaesitas X, Y, Z ita definio:

$$X = z''\cos\vartheta + x''\sin\vartheta, \quad Y = y'', \quad Z = z''\sin\vartheta - x''\cos\vartheta;$$

sic enim utique fiet:

$$X^2 + Y^2 + Z^2 = x''x'' + y''y'' + z''z'' = x'x' + y'y' + z'z' = xx + yy + zz.$$

XV. Ex hac autem triplici positione sequitur fore:

$$x'' = x\cos\zeta + y\sin\zeta, \quad y'' = x\sin\zeta\cos\eta - y\cos\zeta\cos\eta + z\sin\eta,$$
$$z'' = x\sin\zeta\sin\eta - y\cos\zeta\sin\eta - z\cos\eta$$

tum vero

$$X = x(\sin\zeta\sin\eta\cos\vartheta + \cos\zeta\sin\vartheta) - y(\cos\zeta\sin\eta\cos\vartheta - \sin\zeta\sin\vartheta) - z\cos\eta\cos\vartheta$$
$$Y = x\sin\zeta\cos\eta - y\cos\zeta\cos\eta + z\sin\eta$$
$$Z = x(\sin\zeta\sin\eta\sin\vartheta - \cos\zeta\cos\vartheta) - y(\cos\zeta\sin\eta\sin\vartheta + \sin\zeta\cos\vartheta) - z\cos\eta\sin\vartheta,$$

quae formulae cum ante inventis conveniunt.

XVI. Hanc solutionem esse generalem vel inde patet, quod ea complectatur tres angulos arbitrarios ζ, η, ϑ, qui per tres transformationes quas instituimus, sunt introducti. Vis enim hujus methodi in hoc consistit, ut quavis transformatione duae tantum quantitates varientur, dum scilicet in earum locum duae aliae una cum angulo arbitrario introducuntur, tertia manente immutata. Hinc duae operationes jam quidem solutionem problematis suppeditant, sed nondum completam, ob defectum unius quantitatis arbitrariae. Quam ob rem tot transformationes institui oportet, donec tot hujusmodi quantitates arbitrariae fuerint ingressae, quot ad maximam solutionis extensionem requiruntur. Supra autem jam observavi, cum quaestio circa novem numeros versetur, ac tantum sex conditiones praescribantur, tres eorum manere indeterminatos, quemadmodum etiam in solutione hic data ob angulos ζ, η, ϑ arbitrio nostro relictos, tres numeri A, B, D pro lubitu accipi possunt.

XVII. Hinc autem dubium nasci posset, quod cum qualibet transformatione novus angulus introducatur, aucto transformationum numero nostri problematis solutio multo adhuc generalior obtineri posset. Verum tamen qui hujus rei periculum facere voluerit, mox animadvertet, novum angulum introductum cum aliquo praecedentium in unum coalescere, ita ut quotcunque transformationes suscipiantur, numerus angulorum vere arbitrariorum non ultra ternarium augeri queat. Adjiciamus enim insuper hanc transformationem ponendo:

$$X' = X, \quad Y' = Y\cos\lambda - Z\sin\lambda \quad \text{et} \quad Z' = Y\sin\lambda + Z\cos\lambda$$

fietque

$$X' = x(\sin\zeta\sin\eta\cos\vartheta + \cos\zeta\sin\vartheta) + y(\sin\zeta\sin\vartheta - \cos\zeta\cos\eta\cos\vartheta) - z\cos\eta\cos\vartheta,$$
$$Y' = x(\sin\zeta\cos\eta\cos\lambda - \sin\zeta\sin\eta\sin\vartheta\sin\lambda + \cos\zeta\cos\vartheta\sin\lambda)$$
$$- y(\cos\zeta\cos\eta\cos\lambda - \cos\zeta\sin\eta\sin\vartheta\sin\lambda - \sin\zeta\cos\vartheta\sin\lambda)$$
$$+ z(\sin\eta\cos\lambda + \cos\eta\sin\vartheta\sin\lambda),$$

$$Z' = x(\sin\zeta\cos\eta\sin\lambda + \sin\zeta\sin\eta\sin\vartheta\cos\lambda - \cos\zeta\cos\vartheta\cos\lambda)$$
$$- y(\cos\zeta\cos\eta\sin\lambda + \cos\zeta\sin\eta\sin\vartheta\cos\lambda + \sin\zeta\cos\vartheta\cos\lambda)$$
$$+ z(\sin\eta\sin\lambda - \cos\eta\sin\vartheta\cos\lambda),$$

ubi etsi quatuor anguli adsunt ζ, η, ϑ et λ, tamen inde non plures tribus coefficientes pro lubitu assignare licet: quod quidem non facile perspicitur, et nonnisi per plures ambages ostendi posse videtur: cum tamen ex rei natura res sit prorsus manifesta.

XVIII. Etiamsi maxime arduum videatur has quatuor quantitates indeterminatas ad tres revocare, haecque investigatio omnino singulares calculi evolutiones postulet, tamen ratio in eo sita haud difficulter deprehenditur, quod bis inter easdem quantitates cognomines y et z transformatio sit instituta. Scilicet in secunda quantitates y', z' in y'', z'' ope anguli η, et in quarta quantitates cognomines Y et Z ope anguli λ in Y' et Z' sunt transformatae. Quae duae transformationes si immediate se exciperent ponendo exempli gratia

$$\text{primum} \quad y' = y\cos\zeta + z\sin\zeta, \quad z' = y\sin\zeta - z\cos\zeta$$
$$\text{tum vero} \quad y'' = y'\cos\eta + z'\sin\eta, \quad z'' = y'\sin\eta - z'\cos\eta,$$

conjunctim prodiret:

$$y'' = \quad y\cos(\zeta - \eta) + z\sin(\zeta - \eta)$$
$$\text{et} \quad z'' = -y\sin(\zeta - \eta) + z\cos(\zeta - \eta)$$

sicque duplex illa transformatio manifesto unicae, ope anguli $\zeta - \eta$ factae aequivaleret. Quod etiam evenire est intelligendum, etiamsi hujusmodi binae transformationes inter quantitates cognomines non immediate se excipiant.

XIX. Hinc cum quaelibet transformatio inter duas tantum quantitates variabiles instituatur, hanc regulam stabiliri convenit, ut hae transformationes semper inter binas variabiles diversi nominis suscipiantur; quo pacto numerus transformationum ita determinatur, ut plures forent inutiles. Ita cum in nostro problemate tres habeantur quantitates variabiles, litteris x, y, z indicatae, plures quam tres transformationes locum habere nequeunt, dum una inter x et y, alia inter x et z, et tertia inter y et z instituitur hoc modo

$x' = x\cos\zeta + y\sin\zeta$	$x'' = x'\cos\eta + z'\sin\eta$	$x''' = x''$
$y' = x\sin\zeta - y\cos\zeta$	$y'' = y'$	$y''' = y''\cos\vartheta + z''\sin\vartheta$
$z' = z$	$z'' = x'\sin\eta - z'\cos\eta$	$z''' = y''\sin\vartheta - z''\cos\vartheta$

ubi in prima quantitas nominis z, in secunda nominis y, in tertia vero nominis x invariata relinquitur.

XX. Hanc regulam observantes methodum hanc, per istiusmodi transformationes procedentem facile ad ejusmodi problemata accommodare poterimus, quibus plures quam tres quantitates variabiles proponuntur, quas simili modo in alias totidem transformari oporteat, ut quadratorum summa maneat eadem. Pluribus scilicet transformationibus inter binas tantum instituendis opus erit, ubi tantum erit cavendum, ne inter binas cognomines bis transformatio instituatur. Quo observato, solutio non ante erit completa, quam inter omnes binas diversi nominis tales transformationes fuerint absolutae,

cujusmodi diversae combinationes habebuntur sex, si quatuor propositae sint quantitates, decem vero, si quinque, et ita porro. Cujusmodi problemata aliquot cum solutionibus hic subjungam.

Problema. Quatuor quantitates v, x, y, z ita in alias per hujusmodi formulas $\alpha v + \beta x + \gamma y + \delta z$ transformare, ut summa quadratorum maneat eadem, vel ponendo

$$V = Av + Bx + Cy + Dz, \qquad Y = Jv + Kx + Ly + Mz,$$
$$X = Ev + Fx + Gy + Hz, \qquad Z = Nv + Ox + Py + Qz,$$

hos sedecim coefficientes ita definire ut fiat

$$VV + XX + YY + ZZ = vv + xx + yy + zz;$$

quem in finem sequentibus decem conditionibus satisfieri oportet:

$$\begin{array}{llll}
1) & AA + EE + JJ + NN = 1, & 5) & AB + EF + JK + NO = 0,\\
2) & BB + FF + KK + OO = 1, & 6) & AC + EG + JL + NP = 0,\\
3) & CC + GG + LL + PP = 1, & 7) & AD + EH + JM + NQ = 0,\\
4) & DD + HH + MM + QQ = 1, & 8) & BC + FG + KL + OP = 0,\\
 & & 9) & BD + FH + KM + OQ = 0,\\
 & & 10) & CD + GH + LM + PQ = 0.
\end{array}$$

XXI. Cum hic sedecim numeri ex decem conditionibus inveniendi proponantur, evidens est eorum sex arbitrio nostro relinqui, seu quod eodem redit, solutionem completam sex quantitates arbitrarias complecti debere. Methodum autem ante expositam sequentes revera solutionem sex transformationibus absolvi deprehendimus, quae ita repraesentari possunt:

I.	II.	III.
$x' = x\cos\alpha + y\sin\alpha$	$x'' = x'\cos\beta + z'\sin\beta$	$x''' = x''\cos\gamma + v''\sin\gamma$
$y' = x\sin\alpha - y\cos\alpha$	$y'' = y'$	$y''' = y''$
$z' = z$	$z'' = x'\sin\beta - z'\cos\beta$	$z''' = z''$
$v' = v$	$v'' = v'$	$v''' = x''\sin\gamma - v''\cos\gamma$

IV.	V.	VI.
$x^{IV} = x'''$	$x^{V} = x^{IV}$	$x^{VI} = x^{V} \qquad = X$
$y^{IV} = y'''\cos\delta + z'''\sin\delta$	$y^{V} = y^{IV}\cos\varepsilon + v^{IV}\sin\varepsilon$	$y^{VI} = y^{V} \qquad = Y$
$z^{IV} = y'''\sin\delta - z'''\cos\delta$	$z^{V} = z^{IV}$	$z^{VI} = z^{V}\cos\zeta + v^{V}\sin\zeta = Z$
$v^{IV} = v'''$	$v^{V} = y^{IV}\sin\varepsilon - v^{IV}\cos\varepsilon$	$v^{VI} = z^{V}\sin\zeta - v^{V}\cos\zeta = V$

in quas formulas revera sex anguli arbitrarii ingrediuntur, ut solutionis completae indoles postulat.

XXII. Jam perspicuum est ope harum reductionum novas quantitates X, Y, Z, V ita per primum assumtas x, y, z, v expressum iri, ut fiat $X = Ax + By + Cz + Dv$, similiterque etiam reliquae; unde facta evolutione coefficientes ipsarum x, y, z, v in quatuor formis pro X, Y, Z, V oriundis ipsos eos sedecim numeros praebebunt, qui requiruntur pro solutione problematis propositi. Quae cum per se sint manifesta, non opus esse arbitror singulos valores harum sedecim litterarum evolvere. Ceterum cum in harum sex transformationum prima binae litterae x et y, in secunda x

et z, in tertia x et v, in quarta y et z, in quinta y et v et in sexta z et v sint transformatae, quae sunt omnes combinationes possibiles, in hoc ipso etiam continetur criterium solutionis completae.

XXIII. Quoniam autem hic occurrunt quatuor quantitates x, y, z, v in singulis operationibus, duae transformationes binarum institui possunt, quo pacto evolutio valorum quaesitorum non mediocriter sublevatur, uti iterum cavendum ne inter easdem binas litteras plus una transformatione suscipiatur. Sic autem totum negotium tribus operationibus absolvi poterit hoc modo:

I.	II.	III.
$x' = x\cos\alpha + y\sin\alpha$	$x'' = x'\cos\gamma + z'\sin\gamma$	$x''' = x''\cos\varepsilon + v''\sin\varepsilon = X$
$y' = x\sin\alpha - y\cos\alpha$	$y'' = y'\cos\delta + v'\sin\delta$	$y''' = y''\cos\zeta + z''\sin\zeta = Y$
$z' = z\cos\beta + v\sin\beta$	$z'' = x'\sin\gamma - z'\cos\gamma$	$z''' = y''\sin\zeta - z''\cos\zeta = Z$
$v' = z\sin\beta - v\cos\beta$	$v'' = y'\sin\delta - v'\cos\delta$	$v''' = x''\sin\varepsilon - v''\cos\varepsilon = V$

Harum formularum evolutio pro sedecim numeris quaesitis sequentes praebet valores:

$$A = \begin{Bmatrix} +\cos\alpha\cos\gamma\cos\varepsilon \\ +\sin\alpha\sin\delta\sin\varepsilon \end{Bmatrix}, \qquad B = \begin{Bmatrix} +\sin\alpha\cos\gamma\cos\varepsilon \\ -\cos\alpha\sin\delta\sin\varepsilon \end{Bmatrix},$$

$$C = \begin{Bmatrix} +\cos\beta\sin\gamma\cos\varepsilon \\ -\sin\beta\cos\delta\sin\varepsilon \end{Bmatrix}, \qquad D = \begin{Bmatrix} +\sin\beta\sin\gamma\cos\varepsilon \\ +\cos\beta\cos\delta\sin\varepsilon \end{Bmatrix},$$

$$E = \begin{Bmatrix} +\sin\alpha\cos\delta\cos\zeta \\ +\cos\alpha\sin\gamma\sin\zeta \end{Bmatrix}, \qquad F = \begin{Bmatrix} -\cos\alpha\cos\delta\cos\zeta \\ +\sin\alpha\sin\gamma\sin\zeta \end{Bmatrix},$$

$$G = \begin{Bmatrix} +\sin\beta\sin\delta\sin\zeta \\ -\cos\beta\cos\gamma\sin\zeta \end{Bmatrix}, \qquad H = \begin{Bmatrix} -\cos\beta\sin\delta\cos\zeta \\ -\sin\beta\cos\gamma\sin\zeta \end{Bmatrix},$$

$$J = \begin{Bmatrix} +\sin\alpha\cos\delta\sin\zeta \\ -\cos\alpha\sin\gamma\cos\zeta \end{Bmatrix}, \qquad K = \begin{Bmatrix} -\cos\alpha\cos\delta\sin\zeta \\ -\sin\alpha\sin\gamma\cos\zeta \end{Bmatrix},$$

$$L = \begin{Bmatrix} +\sin\beta\sin\delta\sin\zeta \\ +\cos\beta\cos\gamma\cos\zeta \end{Bmatrix}, \qquad M = \begin{Bmatrix} -\cos\beta\sin\delta\sin\zeta \\ +\sin\beta\cos\gamma\cos\zeta \end{Bmatrix},$$

$$N = \begin{Bmatrix} +\cos\alpha\cos\gamma\sin\varepsilon \\ -\sin\alpha\sin\delta\cos\varepsilon \end{Bmatrix}, \qquad O = \begin{Bmatrix} +\sin\alpha\cos\gamma\sin\varepsilon \\ +\cos\alpha\sin\delta\cos\varepsilon \end{Bmatrix},$$

$$P = \begin{Bmatrix} +\cos\beta\sin\gamma\sin\varepsilon \\ +\sin\beta\cos\delta\cos\varepsilon \end{Bmatrix}, \qquad Q = \begin{Bmatrix} +\sin\beta\sin\gamma\sin\varepsilon \\ -\cos\beta\cos\delta\cos\varepsilon \end{Bmatrix},$$

XXIV. Circa hos autem sedecim valores, quibus decem conditiones in problemate allatae implentur, hanc insignem proprietatem locum habere observo, ut iisdem quoque sequentibus decem conditionibus satisfiat:

11) $AA + BB + CC + DD = 1$, 15) $AE + BF + CG + DH = 0$,

12) $EE + FF + GG + HH = 1$, 16) $AJ + BK + CL + DM = 0$,

13) $JJ + KK + LL + MM = 1$, 17) $AN + BO + CP + DQ = 0$,

14) $NN + OO + PP + QQ = 1$, 18) $EJ + FK + GL + HM = 0$,

19) $EN + FO + GP + HQ = 0$,

20) $JN + KO + LP + MQ = 0$.

Quod est theorema prorsus memorabile ac simile ei, quod initio circa novem tantum numeros demonstravi. Eo autem modo, quo ibi demonstrationem adornavi, hic quidem ob litterarum multitudinem uti non licebit; sed quoniam ad hos valores generales successive pervenire docui, demonstratio ita convenientissime conficietur, ut si haec proprietas in valoribus quibusque antecedentibus locum habuerit, eadem quoque in sequentibus, per transformationem inde derivatis locum habere ostendatur.

XXV. Consideremus igitur valores quoscunque intermedios qui per quatuor primitivas quantitates x, y, z, v ita definiantur, ut sit

$$x^{(n)} = \mathfrak{A}x + \mathfrak{B}y + \mathfrak{C}z + \mathfrak{D}v, \qquad y^{(n)} = \mathfrak{E}x + \mathfrak{F}y + \mathfrak{G}z + \mathfrak{H}v,$$
$$z^{(n)} = \mathfrak{J}x + \mathfrak{K}y + \mathfrak{L}z + \mathfrak{M}v, \qquad v^{(n)} = \mathfrak{N}x + \mathfrak{O}y + \mathfrak{P}z + \mathfrak{Q}v,$$

ubi coefficientes ita sint comparati, ut supra memoratis conditionibus satisfaciant; scilicet ut sit:

$$\mathfrak{A}\mathfrak{A} + \mathfrak{B}\mathfrak{B} + \mathfrak{C}\mathfrak{C} + \mathfrak{D}\mathfrak{D} = 1, \qquad \mathfrak{A}\mathfrak{E} + \mathfrak{B}\mathfrak{F} + \mathfrak{C}\mathfrak{G} + \mathfrak{D}\mathfrak{H} = 0,$$
$$\mathfrak{E}\mathfrak{E} + \mathfrak{F}\mathfrak{F} + \mathfrak{G}\mathfrak{G} + \mathfrak{H}\mathfrak{H} = 1, \qquad \mathfrak{A}\mathfrak{J} + \mathfrak{B}\mathfrak{K} + \mathfrak{C}\mathfrak{L} + \mathfrak{D}\mathfrak{M} = 0,$$
$$\mathfrak{J}\mathfrak{J} + \mathfrak{K}\mathfrak{K} + \mathfrak{L}\mathfrak{L} + \mathfrak{M}\mathfrak{M} = 1, \qquad \mathfrak{A}\mathfrak{N} + \mathfrak{B}\mathfrak{O} + \mathfrak{C}\mathfrak{P} + \mathfrak{D}\mathfrak{Q} = 0,$$
$$\mathfrak{N}\mathfrak{N} + \mathfrak{O}\mathfrak{O} + \mathfrak{P}\mathfrak{P} + \mathfrak{Q}\mathfrak{Q} = 1, \qquad \mathfrak{E}\mathfrak{J} + \mathfrak{F}\mathfrak{K} + \mathfrak{G}\mathfrak{L} + \mathfrak{H}\mathfrak{M} = 0,$$
$$\mathfrak{E}\mathfrak{N} + \mathfrak{F}\mathfrak{O} + \mathfrak{G}\mathfrak{P} + \mathfrak{H}\mathfrak{Q} = 0,$$
$$\mathfrak{J}\mathfrak{N} + \mathfrak{K}\mathfrak{O} + \mathfrak{L}\mathfrak{P} + \mathfrak{M}\mathfrak{Q} = 0,$$

quae conditiones utique in prima positione locum habent, ubi est $x^{(n)} = x$, $y^{(n)} = y$, $z^{(n)} = z$, $v^{(n)} = v$; siquidem tum habetur:

$$\mathfrak{A} = 1, \quad \mathfrak{E} = 0, \quad \mathfrak{J} = 0, \quad \mathfrak{N} = 0,$$
$$\mathfrak{B} = 0, \quad \mathfrak{F} = 1, \quad \mathfrak{K} = 0, \quad \mathfrak{O} = 0,$$
$$\mathfrak{C} = 0, \quad \mathfrak{G} = 0, \quad \mathfrak{L} = 1, \quad \mathfrak{P} = 0,$$
$$\mathfrak{D} = 0, \quad \mathfrak{H} = 0, \quad \mathfrak{M} = 0, \quad \mathfrak{Q} = 1.$$

XXVI. Ponamus ex illis valoribus per transformationem sequentes ita derivari

ut posito	prodeant hi valores derivati:
$x^{(n+1)} = x^{(n)} \cos\vartheta + y^{(n)} \sin\vartheta$	$x^{(n+1)} = \mathfrak{A}'x + \mathfrak{B}'y + \mathfrak{C}'z + \mathfrak{D}'v$
$y^{(n+1)} = x^{(n)} \sin\vartheta - y^{(n)} \cos\vartheta$	$y^{(n+1)} = \mathfrak{E}'x + \mathfrak{F}'y + \mathfrak{G}'z + \mathfrak{H}'v$
$z^{(n+1)} = z^{(n)}$	$z^{(n+1)} = \mathfrak{J}'x + \mathfrak{K}'y + \mathfrak{L}'z + \mathfrak{M}'v$
$v^{(n+1)} = v^{(n)}$	$v^{(n+1)} = \mathfrak{N}'x + \mathfrak{O}'y + \mathfrak{P}'z + \mathfrak{Q}'v$

eritque:

$$\mathfrak{A}' = \mathfrak{A}\cos\vartheta + \mathfrak{E}\sin\vartheta, \quad \mathfrak{E}' = \mathfrak{A}\sin\vartheta - \mathfrak{E}\cos\vartheta, \quad \mathfrak{J}' = \mathfrak{J}, \quad \mathfrak{N}' = \mathfrak{N},$$
$$\mathfrak{B}' = \mathfrak{B}\cos\vartheta + \mathfrak{F}\sin\vartheta, \quad \mathfrak{F}' = \mathfrak{B}\sin\vartheta - \mathfrak{F}\cos\vartheta, \quad \mathfrak{K}' = \mathfrak{K}, \quad \mathfrak{O}' = \mathfrak{O},$$
$$\mathfrak{C}' = \mathfrak{C}\cos\vartheta + \mathfrak{G}\sin\vartheta, \quad \mathfrak{G}' = \mathfrak{C}\sin\vartheta - \mathfrak{G}\cos\vartheta, \quad \mathfrak{L}' = \mathfrak{L}, \quad \mathfrak{P}' = \mathfrak{P},$$
$$\mathfrak{D}' = \mathfrak{D}\cos\vartheta + \mathfrak{H}\sin\vartheta, \quad \mathfrak{H}' = \mathfrak{D}\sin\vartheta - \mathfrak{H}\cos\vartheta, \quad \mathfrak{M}' = \mathfrak{M}, \quad \mathfrak{Q}' = \mathfrak{Q}.$$

Unde quidem hae conditiones jam sponte implentur:

$$\mathfrak{J}'\mathfrak{J}' + \mathfrak{K}'\mathfrak{K}' + \mathfrak{L}'\mathfrak{L}' + \mathfrak{M}'\mathfrak{M}' = 1, \qquad \mathfrak{J}'\mathfrak{N}' + \mathfrak{K}'\mathfrak{O}' + \mathfrak{L}'\mathfrak{P}' + \mathfrak{M}'\mathfrak{Q}' = 0,$$
$$\mathfrak{N}'\mathfrak{N}' + \mathfrak{O}'\mathfrak{O}' + \mathfrak{P}'\mathfrak{P}' + \mathfrak{Q}'\mathfrak{Q}' = 1.$$

XXVII. Reliquis vero etiam conditionibus satisfieri facile ostenditur; erit enim:

$$\mathfrak{A}'\mathfrak{A}'+\mathfrak{B}'\mathfrak{B}'+\mathfrak{C}'\mathfrak{C}'+\mathfrak{D}'\mathfrak{D}'=\left\{\begin{array}{l} +\ (\mathfrak{A}\mathfrak{A}+\mathfrak{B}\mathfrak{B}+\mathfrak{C}\mathfrak{C}+\mathfrak{D}\mathfrak{D})\cos^2\vartheta \\ +\ (\mathfrak{E}\mathfrak{E}+\mathfrak{F}\mathfrak{F}+\mathfrak{G}\mathfrak{G}+\mathfrak{H}\mathfrak{H})\sin^2\vartheta \\ +2(\mathfrak{A}\mathfrak{E}+\mathfrak{B}\mathfrak{F}+\mathfrak{C}\mathfrak{G}+\mathfrak{D}\mathfrak{H})\sin\vartheta\cos\vartheta \end{array}\right.$$

$$=+1.\cos^2\vartheta+1.\sin^2\vartheta+0.\sin\vartheta\cos\vartheta=1,$$

quod simili modo de summa quadratorum secundae columnae $\mathfrak{E}'\mathfrak{E}'+\mathfrak{F}'\mathfrak{F}'+\mathfrak{G}'\mathfrak{G}'+\mathfrak{H}'\mathfrak{H}'$ ostenditur. Deinde etiam res manifesta est circa summam productorum:

$$\mathfrak{A}'\mathfrak{J}'+\mathfrak{B}'\mathfrak{K}'+\mathfrak{C}'\mathfrak{L}'+\mathfrak{D}'\mathfrak{M}'=-(\mathfrak{A}\mathfrak{J}+\mathfrak{B}\mathfrak{K}+\mathfrak{C}\mathfrak{L}+\mathfrak{D}\mathfrak{M})\cos\vartheta+(\mathfrak{E}\mathfrak{J}+\mathfrak{F}\mathfrak{K}+\mathfrak{G}\mathfrak{L}+\mathfrak{H}\mathfrak{M})\sin\vartheta=0$$

pariterque etiam circa has summas:

$$\mathfrak{A}'\mathfrak{N}'+\mathfrak{B}'\mathfrak{O}'+\mathfrak{C}'\mathfrak{P}'+\mathfrak{D}'\mathfrak{Q}'=0,\qquad \mathfrak{E}'\mathfrak{J}'+\mathfrak{F}'\mathfrak{K}'+\mathfrak{G}'\mathfrak{L}'+\mathfrak{H}'\mathfrak{M}'=0$$

$$\text{et}\quad \mathfrak{E}'\mathfrak{N}'+\mathfrak{F}'\mathfrak{O}'+\mathfrak{G}'\mathfrak{P}'+\mathfrak{H}'\mathfrak{Q}'=0$$

unde tantum relinquitur haec:

$$\mathfrak{A}'\mathfrak{E}'+\mathfrak{B}'\mathfrak{F}'+\mathfrak{C}'\mathfrak{G}'+\mathfrak{D}'\mathfrak{H}'=\left\{\begin{array}{l} +(\mathfrak{A}\mathfrak{A}+\mathfrak{B}\mathfrak{B}+\mathfrak{C}\mathfrak{C}+\mathfrak{D}\mathfrak{D})\sin\vartheta\cos\vartheta \\ -(\mathfrak{E}\mathfrak{E}+\mathfrak{F}\mathfrak{F}+\mathfrak{G}\mathfrak{G}+\mathfrak{H}\mathfrak{H})\sin\vartheta\cos\vartheta \\ +(\mathfrak{A}\mathfrak{E}+\mathfrak{B}\mathfrak{F}+\mathfrak{C}\mathfrak{G}+\mathfrak{D}\mathfrak{H})\sin^2\vartheta \\ -(\mathfrak{A}\mathfrak{E}+\mathfrak{B}\mathfrak{F}+\mathfrak{C}\mathfrak{G}+\mathfrak{D}\mathfrak{H})\cos^2\vartheta \end{array}\right.$$

$$=+\sin\vartheta\cos\vartheta-\sin\vartheta\cos\vartheta+0.\sin^2\vartheta-0.\cos^2\vartheta=0.$$

XXVIII. Cum igitur harum decem conditionum veritas in positione prima, uti jam ostendi, sit manifesta, etiam in positione secunda per transformationem binarum inde deducta quoque subsistet, hincque etiam in omnibus sequentibus positionibus simili modo ex praecedentibus deductis. Quocirca etiam solutio generalis sex transformationibus, uti in § XXI, absoluta ita erit comparata, ut non solum decem conditionibus in problemate praescriptis, sed etiam alteris illis decem § XXIV commemoratis satisfaciat: hocque ita ut decem prioribus conditionibus satisfieri nequeat, quin simul decem posterioribus satisfiat. Atque hinc jam facile colligitur eandem proprietatem etiam in problematibus, ubi similis quaestio circa 25, 36 pluresque numeros instituitur, semper locum habere debere. Progredior igitur ad sequens

Problema. Invenire 25 numeros A, B, C, D, etc. ita in formam quadrati disponendos:

$$\begin{array}{ccccc} A, & B, & C, & D, & E, \\ F, & G, & H, & J, & K, \\ L, & M, & N, & O, & P, \\ Q, & R, & S, & T, & U, \\ V, & W, & X, & Y, & Z, \end{array}$$

ut summae quadratorum ex singulis columnis tam verticalibus quam horizontalibus desumtorum unitati aequentur, summae productorum autem ex binis columnis sive verticalibus, sive horizontalibus formatorum evanescant.

XXIX. Ex praecedentibus intelligitur hoc problema eo reduci, ut sumtis istis 25 numeris pro coefficientibus, quinque variabiles u, v, x, y, z per hujusmodi formulas in alias transformentur:

$$U = Au + Bv + Cx + Dy + Ez$$
$$V = Fu + Gv + Hx + Jy + Kz$$
$$X = Lu + Mv + Nx + Oy + Pz$$
$$Y = Qu + Rv + Sx + Ty + Uz$$
$$Z = Vu + Wv + Xx + Yy + Zz$$

ut fiat:

$$UU + VV + XX + YY + ZZ = uu + vv + xx + yy + zz.$$

Quod ergo problema, cum quinque quantitates decem combinationes diversas binarum admittant, per decem transformationes successive in binis instituendas, resolvetur, hoc modo:

I.

$$u' = u\cos\alpha + v\sin\alpha$$
$$v' = u\sin\alpha - v\cos\alpha$$
$$x' = x$$
$$y' = y$$
$$z' = z$$

II.

$$u'' = u'\cos\beta + x'\sin\beta$$
$$v'' = v'$$
$$x'' = u'\sin\beta - x'\cos\beta$$
$$y'' = y'$$
$$z'' = z'$$

III.

$$u''' = u''\cos\gamma + y''\sin\gamma$$
$$v''' = v''$$
$$x''' = x''$$
$$y''' = u''\sin\gamma - y''\cos\gamma$$
$$z''' = z''$$

IV.

$$u^{IV} = u'''\cos\delta + z'''\sin\delta$$
$$v^{IV} = v'''$$
$$x^{IV} = x'''$$
$$y^{IV} = y'''$$
$$z^{IV} = u'''\sin\delta - z'''\cos\delta$$

V.

$$u^{V} = u^{IV}$$
$$v^{V} = v^{IV}\cos\varepsilon + x^{IV}\sin\varepsilon$$
$$x^{V} = v^{IV}\sin\varepsilon - x^{IV}\cos\varepsilon$$
$$y^{V} = y^{IV}$$
$$z^{V} = z^{IV}$$

VI.

$$u^{VI} = u^{V}$$
$$v^{VI} = v^{V}\cos\zeta + y^{V}\sin\zeta$$
$$x^{VI} = x^{V}$$
$$y^{VI} = v^{V}\sin\zeta - y^{V}\cos\zeta$$
$$z^{VI} = z^{V}$$

VII.

$$u^{VII} = u^{VI}$$
$$v^{VII} = v^{VI}\cos\eta + z^{VI}\sin\eta$$
$$x^{VII} = x^{VI}$$
$$y^{VII} = y^{VI}$$
$$z^{VII} = v^{VI}\sin\eta - z^{VI}\cos\eta$$

VIII.

$$u^{VIII} = u^{VII}$$
$$v^{VIII} = v^{VII}$$
$$x^{VIII} = x^{VII}\cos\vartheta + y^{VII}\sin\vartheta$$
$$y^{VIII} = x^{VII}\sin\vartheta - y^{VII}\cos\vartheta$$
$$z^{VIII} = z^{VII}$$

IX.

$$u^{IX} = u^{VIII}$$
$$v^{IX} = v^{VIII}$$
$$x^{IX} = x^{VIII}\cos\varkappa + z^{VIII}\sin\varkappa$$
$$y^{IX} = y^{VIII}$$
$$z^{IX} = x^{VIII}\sin\varkappa - z^{VIII}\cos\varkappa$$

X.

$$u^{X} = u^{IX} = U$$
$$v^{X} = v^{IX} = V$$
$$x^{X} = x^{IX} = X$$
$$y^{X} = y^{IX}\cos\lambda + z^{IX}\sin\lambda = Y$$
$$z^{X} = y^{IX}\sin\lambda - z^{IX}\cos\lambda = Z$$

XXX. His ergo operationibus decem anguli arbitrarii introducuntur, in quo character solutionis completae seu generalis consistit. Cum enim conditiones ex columnis verticalibus petitae problemati solvendo sufficiant, indeque alterae conditiones ad columnas horizontales spectantes sponte impleantur,

quadratorum summae praebent quinque, producta vero ex binis decem aequationes; ita ut omnino 15 conditionibus sit satisfaciendum; quare cum 25 numeri investigandi proponantur, ex iis decem adhuc manebunt indeterminati, in quo etiam solutio hic data egregie consentit, dum plures quam decem transformationes, quae quidem circa binas quantitates diversas instituantur, locum habere nequeunt.

XXXI. Quo illarum formularum evolutio facilior reddatur, qualibet operatione duae transformationes conjungi possunt, prorsus ut in solutione praecedentis problematis est factum. Has autem conjunctiones ita capi convenit, ut quantitas solitaria nullam mutationem patiens in omnibus sit diversa: id quod evenit si binae praecedentium transformationum hoc modo conjungantur:

(I, VIII), (II, VII), (III, IX), (IV, VI), (V, X)

unde sequentes quinque transformationes oriuntur:

I.

$$\begin{aligned} u' &= u\cos\alpha + v\sin\alpha \\ v' &= u\sin\alpha - v\cos\alpha \\ x' &= x\cos\beta + y\sin\beta \\ y' &= x\sin\beta - y\cos\beta \\ z' &= z \end{aligned}$$

II.

$$\begin{aligned} u'' &= u'\cos\gamma + x'\sin\gamma \\ v'' &= v'\cos\delta + z'\sin\delta \\ x'' &= u'\sin\gamma - x'\cos\gamma \\ y'' &= y' \\ z'' &= v'\sin\delta - z'\cos\delta \end{aligned}$$

III.

$$\begin{aligned} u''' &= u''\cos\varepsilon + y''\sin\varepsilon \\ v''' &= v'' \\ x''' &= x''\cos\zeta + z''\sin\zeta \\ y''' &= u''\sin\varepsilon - y''\cos\varepsilon \\ z''' &= x''\sin\zeta - z''\cos\zeta \end{aligned}$$

IV.

$$\begin{aligned} u^{IV} &= u'''\cos\eta + z'''\sin\eta \\ v^{IV} &= v'''\cos\vartheta + y'''\sin\vartheta \\ x^{IV} &= x''' \\ y^{IV} &= v'''\sin\vartheta - y'''\cos\vartheta \\ z^{IV} &= u'''\sin\eta - z'''\cos\eta \end{aligned}$$

V.

$$\begin{aligned} u^{V} &= u^{IV} \\ v^{V} &= v^{IV}\cos\varkappa + x^{IV}\sin\varkappa \\ x^{V} &= v^{IV}\sin\varkappa - z^{IV}\cos\varkappa \\ y^{V} &= y^{IV}\cos\lambda + z^{IV}\sin\lambda \\ z^{V} &= y^{IV}\sin\lambda - z^{IV}\cos\lambda. \end{aligned}$$

XXXII. Simili modo problemata hujus generis circa 36 pluresque numeros, quorum quidem multitudo est numerus quadratus, resolvi possunt; ubi pro calculo contrahendo non solum duas, sed etiam tres ac deinceps plures transformationes in una operatione complecti licebit; atque hic perpetuo pulcherrimus consensus inter solutionem generalem ex omnibus combinationibus eliciendam ac rei naturam deprehendetur. Posito enim in genere quantitatum quaesitarum numero $= nn$, quadratorum summae unitati aequandae praebent n conditiones, productorum autem ex binis nihilo aequandae $\frac{nn-n}{2}$, sicque conjunctim $\frac{nn+n}{2}$ conditiones, quo numero a numero quaesitorum nn ablato, restat $\frac{nn-n}{2}$, ac propterea totidem ex quaesitis manebunt indeterminati, seu solutio generalis totidem quantitates arbitrarias complecti debet, secundum regulam autem supra expositam in hunc finem $\frac{nn-n}{2}$ transformationibus est utendum, quibus ergo praecise tot anguli arbitrarii in calculum introducuntur.

Problematis initio propositi solutio generalis in numeris rationalibus.

XXXIII. Coronidis loco solutionem problematis nostri, e methodo Diophantea petitam, subjungam, quae sequenti modo satis concinne exhiberi potest.

Sumantur pro lubitu quatuor numeri p, q, r, s, ac posita quadratorum eorum summa

$$pp + qq + rr + ss = u$$

novem numeri quaesiti ita determinati reperiuntur:

$$A = \frac{pp + qq - rr - ss}{u}, \qquad B = \frac{2qr + 2ps}{u}, \qquad C = \frac{2qs - 2pr}{u},$$

$$D = \frac{2qr - 2ps}{u}, \qquad E = \frac{pp - qq + rr - ss}{u}, \qquad F = \frac{2pq + 2rs}{u},$$

$$G = \frac{2qs + 2pr}{u}, \qquad H = \frac{2rs - 2pq}{u}, \qquad J = \frac{pp - qq - rr + ss}{u}.$$

Hinc simplicissimi numeri, qui quidem inter se omnes sint inaequales, colliguntur sequentes in quadratum dispositi:

$+\frac{47}{57}$	$+\frac{28}{57}$	$-\frac{16}{57}$
$+\frac{4}{57}$	$+\frac{23}{57}$	$+\frac{52}{57}$
$+\frac{32}{57}$	$-\frac{44}{57}$	$+\frac{17}{57}$

hic est $p = 6$, $q = 4$, $r = 2$, $s = 1$.

$+\frac{53}{63}$	$+\frac{26}{63}$	$-\frac{22}{63}$
$-\frac{2}{63}$	$+\frac{43}{63}$	$+\frac{46}{63}$
$+\frac{34}{63}$	$-\frac{38}{63}$	$+\frac{37}{63}$

ubi est $p = 7$, $q = 3$, $r = 2$, $s = 1$.

En adhuc alia fere aeque simplicia exempla

$+\frac{53}{71}$	$-\frac{42}{71}$	$+\frac{26}{71}$
$-\frac{18}{71}$	$+\frac{19}{71}$	$+\frac{66}{71}$
$+\frac{46}{71}$	$+\frac{54}{71}$	$-\frac{3}{71}$

$+\frac{86}{99}$	$+\frac{38}{99}$	$-\frac{31}{99}$
$-\frac{14}{99}$	$+\frac{79}{99}$	$+\frac{58}{99}$
$+\frac{47}{99}$	$-\frac{46}{99}$	$+\frac{74}{99}$

Pro casu sedecim numerorum.

XXXIV. Si pro casu sedecim numerorum, simili modo in quadratum disponendorum, solutio in rationalibus desideretur, unde facile numeros non nimis magnos reperire liceat, methodus supra data ad hunc finem difficulter accommodatur. Alio autem modo, prorsus singulari, sequentem solutionem latissime patentem sum nactus, ubi sumtis pro lubitu octo numeris a, b, c, d, p, q, r, s, sedecim numeri in quadratum dispositi ita se habent

$+ap + bq + cr + ds$	$+aq - bp + cs - dr$	$+ar - bs - cp + dq$	$+as + br - cq - dp$
$+aq - bp - cs + dr$	$-ap - bq + cr + ds$	$-as - br - cq - dp$	$+ar - bs + cp - dq$
$+ar + bs - cp - dq$	$+as - br - cq + dp$	$-ap + bq - cr + ds$	$-aq - bp - cs - dr$
$+as - br + cq - dp$	$-ar - bs - cp - dq$	$+aq + bp - cs - dr$	$-ap + bq + cr - ds$

ubi summa quadratorum in singulis columnis sive horizontalibus sive verticalibus prodit ubique eadem

$$= (aa + bb + cc + dd)(pp + qq + rr + ss).$$

Quare ut hae summae unitati aequentur, hanc expressionem quadratum reddi, per ejusque radicem singulos numeros dividi oportet. Tum vero hi sedecim numeri etiam hac gaudent proprietate, ut summa productorum ex binis columnis sive horizontalibus, sive verticalibus sumtorum ubique evanescat.

XXXV. Hinc ergo facile plurima exempla in numeris satis exiguis deduci possunt, inter quae sequens ideo notatu dignum videtur, quod omnes numeri sint inter se inaequales:

Numeri:

+37	+ 4	+ 1	+12
− 6	+33	−18	+ 9
+11	+ 8	− 7	−36
− 2	+19	+34	− 3

Quadrata:

				Summae
	1369	16	1	144	= 1530
	36	1089	324	81	= 1530
	121	64	49	1296	= 1530
	4	361	1156	9	= 1530
Summae.	1530	1530	1530	1530	

ac de productis binorum res est manifesta:

$$\text{cum sit} \qquad -6.37 + 4.33 - 1.18 + 9.12 = 0$$

$$+4.37 - 6.33 + 8.11 - 2.19 = 0.$$

etc.

Generales autem formas inspicienti facile patebit, per eas omnes illas 20 conditiones §§ XX et XXIV allatas perfecte impleri, siquidem summae quaternorum quadratorum ad unitatem revocentur.

XXXVI. Solutio haec eo majorem attentionem meretur, quod ad eam nulla certa methodo, sed potius quasi divinando sum perductus: et quoniam ea adeo octo numeros arbitrarios implicat, qui quidem facta reductione ad unitatem, ad septem rediguntur, vix dubitare licet, quin ista solutio sit universalis et omnes prorsus solutiones possibiles in se complectatur. Si quis ergo viam directam ad hanc solutionem manuducentem investigaverit, insignia certe subsidia analysi attulisse erit censendus. Utrum autem similes solutiones pro amplioribus quadratis, quae numeris 25, 36 et majoribus constant, expectare liceat, vix affirmare ausim. Non solum autem hinc algebra communis, sed etiam methodus Diophantea maxima incrementa adeptura videtur.

Problema curiosum.

Invenire sedecim numeros ita in quadratum disponendos,

$$\begin{matrix} A, & B, & C, & D, \\ E, & F, & G, & H, \\ J, & K, & L, & M, \\ N, & O, & P, & Q, \end{matrix}$$

ut non solum summae quadratorum per columnas tam horizontales quam verticales sumtorum, sed etiam eae, quae per diagonales sumuntur, scilicet

$$A^2 + F^2 + L^2 + Q^2 \quad \text{et} \quad D^2 + G^2 + K^2 + N^2$$

sint omnes inter se aequales, ac praeterea producta binorum ita sumtorum, ut supra est praeceptum, evanescant, scilicet

$AE + BF + CG + DH = 0$	$AB + EF + JK + NO = 0$
$AJ + BK + CL + DM = 0$	$AC + EG + JL + NP = 0$
$AN + BO + CP + DQ = 0$	$AD + EH + JM + NQ = 0$
$EJ + FK + GL + HM = 0$	$BC + FG + KL + OP = 0$
$EN + FO + GP + HQ = 0$	$BD + FH + KM + OQ = 0$
$JN + KO + LP + MQ = 0$	$CD + GH + LM + PQ = 0.$

Solutio.

Hic ergo proponuntur 22 conditiones, quibus satisfieri oportet; omissis autem duabus ad diagonales spectantibus, sequens forma generalis reliquas omnes adimplet:

$+ap+bq+cr+ds$	$+ar-bs-cp+dq$	$-as-br+cq+dp$	$+aq-bp+cs-dr$
$-aq+bp+cs-dr$	$+as+br+cq+dp$	$+ar-bs+cp-dq$	$+ap+bq-cr-ds$
$+ar+bs-cp-dq$	$-ap+bq-cr+ds$	$+aq+bp+cs+dr$	$+as-br-cq+dp$
$-as+br-cq+dp$	$-aq-bp+cs+dr$	$-ap+bq+cr-ds$	$+ar+bs+cp+dq$

ubi summa quaternorum quadratorum ex columnis tam horizontalibus quam verticalibus sumtorum est

$$(aa+bb+cc+dd)(pp+qq+rr+ss)$$

cui ut etiam summae quadratorum per diagonales sumtorum aequentur, sequentes binas aequationes confici oportet:

$$+abpq+abrs+acpr+acqs+adps+adqr+bcqr+bcps+bdqs+bdpr+cdrs+cdpq=0,$$
$$-abpq-abrs+acpr+acqs-adps-adqr-bcqr-bcps+bdqs+bdpr-cdrs-cdpq=0,$$

ex quibus deducuntur hae duae:

$$(ac+bd)(pr+qs)=0$$
$$(ab+cd)(pq+rs)+(ad+bc)(ps+qr)=0.$$

Unde hae duae determinationes eliciuntur:

$$\text{I.}\quad pr+qs=0 \quad \text{et} \quad \text{II.}\quad \frac{a}{c}=\frac{-d(pq+rs)-b(ps+qr)}{b(pq+rs)+d(ps+qr)}$$

ita ut adhuc sex litterae arbitrio nostro relinquantur.

Evolvamus exemplum sumendo $p=6$, $q=3$, $r=1$, $s=-2$, unde cum fiat $\frac{a}{c}=\frac{-16d+9b}{16b-9d}$, sit $d=0$, $b=1$, $a=9$, $c=16$, et quadratum omnibus conditionibus satisfaciens erit

$+73$	-85	$+65$	-11
-53	$+31$	$+107$	$+41$
-89	-67	$+1$	-67
-29	-65	-35	$+103$

ubi summae quaternorum quadratorum secundum columnas tam horizontales quam verticales, itidemque secundum diagonales sumtorum, prodeunt = 16900, ex quo si hi numeri dividerentur per 130, hae summae omnes ad unitatem redigerentur.

Si quem hic offendant numeri 65 et 67 bis occurrentes, adjungam aliud hujusmodi quadratum minoribus adeo numeris expressum:

+ 68	− 29	+ 41	− 37
− 17	+ 31	+ 79	+ 32
+ 59	+ 28	− 23	+ 61
− 11	− 77	+ 8	+ 49

ubi quaternorum quadratorum summa est 8515.

Notetur denique in his quadratis etiam quadrata tam quatuor numerorum angularium, quam quatuor mediorum eandem summam producere.



XXXI.

Solutio quorundam problematum Diophanteorum.

(N. Comment. XX. 1775. p. 48. Exhib. 1771 Jul. 4.)

Problema I. Invenire duo quadratorum paria xx, yy et tt, uu, ita ut tam $(xx+yy)(ttxx+uuyy)$ quam $(xx+yy)(uuxx+ttyy)$ fiat numerus quadratus.

1. **Analysis.** Primo patet, quicunque bini numeri tam pro x, y, quam pro t, u fuerint inventi, eorum aeque multipla, veluti αx, αy et βt, βu quaesito aeque satisfacere; sicque problema ita restringi conveniet, ut tam x et y quam t et u sint numeri primi inter se.

2. Incipiamus a formula priori $(xx+yy)(ttxx+uuyy)$, quae posita huic quadrato

$$(xx+yy)^2 xxyy(pp+qq)^2$$

aequalis, fit

$$ttxx+uuyy = xxyy(xx+yy)((pp-qq)^2+(2pq)^2)$$

unde concluditur

$$tx = xy(x(pp-qq)+2pqy), \quad uy = xy(y(pp-qq)-2pqx)$$

sicque erit

$$t = xy(pp-qq)+2pqyy, \quad u = xy(pp-qq)-2pqxx.$$

3. Jam pro altera formula, cum sit

$$ty = xyy(pp-qq)+2pqy^3, \quad ux = xxy(pp-qq)-2pqx^3$$

fiet

$$ttyy+uuxx = xxy^4(pp-qq)^2+4pqxy^5(pp-qq)+4ppqqy^6+x^4yy(pp-qq)^2-4pqx^5y(pp-qq)+4ppqqx^6$$

quae forma, quia manifesto per $xx+yy$ est divisibilis, abit in

$$(xx+yy)(xxyy(pp-qq)^2-4pqxy(xx-yy)(pp-qq)+4ppqq(x^4-xxyy+y^4))$$

4. Cum nunc haec forma per $xx+yy$ multiplicata numerum quadratum praebere debeat, habebimus sequentem expressionem ad quadratum reducendam:

$$4ppqqx^4-4pq(pp-qq)x^3y+(p^4-6p^2q^2+q^4)x^2y^2+4pq(pp-qq)xy^3+4ppqqy^4$$

quae quidem manifesto fit quadratum, si $x=y$; verum hunc casum utpote facillimum hinc merito excludimus; siquidem tota quaestio huc rediret, ut $2(tt+uu)$ quadratum efficeretur.

5. At ponendo illam formulam aequalem huic quadrato

$$(2pqxx-(pp-qq)xy+2pqyy)^2$$

deletis terminis paribus fit

$$(p^4-6ppqq+q^4)x^2y^2+4pq(pp-qq)xy^3 = (p^4+6ppqq+q^4)x^2y^2-4pq(pp-qq)xy^3$$

hincque $8pq(pp-qq)y = 12ppqqx$; unde colligitur haec solutio problematis:

$x = 2(pp-qq)$, $y = 3pq$, hincque porro $t = 6pq(p^4+ppqq+q^4)$ et $u = -2pq(pp-qq)^2$.

6. En ergo solutionem primam infinite patentem, quoniam numeros p et q ad arbitrium capere licet; reductis scilicet numeris t et u ad minimos terminos, et quia perinde est sive sint positivi sive negativi, habebimus

$$x = 2(pp - qq), \quad t = 3(p^4 + ppqq + q^4) = \tfrac{3}{4}xx + yy$$
$$y = 3pq, \quad u = (pp - qq)^2 = \tfrac{1}{4}xx$$

hincque reperitur

$$xx + yy = 4p^4 + ppqq + 4q^4$$
$$ttxx + uuyy = xxyy(xx + yy)(pp + qq)^2 = xx(xx + yy)(\tfrac{9}{16}xx + yy)$$
$$uuxx + ttyy = 4ppqq(xx + yy)(p^4 + 7ppqq + q^4)^2 = (xx + yy)(\tfrac{1}{4}xx + yy)^2.$$

7. Ut alias solutiones inveniamus, ponamus superioris formae radicem quadratam:

$$2ppxx - (pp - qq)xy - 2pqyy + Ayy$$

cujus quadrato illi aequali posito prodibit aequatio:

$$(AA - 4Apq)yy - 2A(pp - qq)xy + (4Apq - 4ppqq)xx = 0$$

hic si $A = 4pq$, prodit solutio praecedens; at posito $A = pq$ fit

$$+ 3pqy + 2(pp - qq)x = 0,$$

quae cum illa pariter congruit.

8. Ponamus $A = -2pp$ prodibitque haec aequatio

$$(pp + 2pq)yy + (pp - qq)xy - (2pq + qq)xx = 0,$$

quae per $x + y$ divisa dat

$$(pp + 2pq)y - (2pq + qq)x = 0$$

unde fit $\quad x = p(p + 2q) \quad$ et $\quad y = q(q + 2p)$

tum vero $\quad t = ppq(q + 2p)(pp + 2pq + 3qq) \quad$ et $\quad u = pqq(p + 2q)(qq + 2pq + 3pp)$.

9. En ergo aliam solutionem a praecedente diversam, et infinite patentem, qua numeris t et u ad minimos terminos reductis fit

$$x = p(p + 2q), \quad t = p(q + 2p)(pp + 2pq + 3qq)$$
$$y = q(q + 2p), \quad u = q(p + 2q)(qq + 2pq + 3pp)$$

hincque reperitur:

$$xx + yy = p^4 + 4p^3q + 8ppqq + 4pq^3 + q^4$$
$$ttxx + uuyy = (p + 2q)^2(q + 2p)^2(pp + qq)^2(xx + yy)$$
$$uuxx + ttyy = ppqq(5pp + 8pq + 5qq)^2(xx + yy).$$

10. Posito $A = 2pp$ prodit $(pp - 2pq)yy - (pp - qq)xy + (2pq - qq)xx = 0$, quae per $y - x$ divisa dat $(pp - 2pq)y - (2pq - qq)x = 0$, ideoque

$$x = p(p - 2q), \quad t = p(2p - q)(pp - 2pq + 3qq)$$
$$y = q(2p - q), \quad u = q(p - 2q)(qq - 2pq + 3qq)$$
$$xx + yy = p^4 - 4p^3q + 8ppqq - 4pq^3 + q^4$$
$$ttxx + uuyy = (p - 2q)^2(2p - q)^2(pp + qq)^2(xx + yy)$$
$$uuxx + ttyy = ppqq(5pp - 8pq + 5qq)^2(xx + yy).$$

Haec autem solutio a praecedente non differt; neque positiones $A = 2qq$ et $A = -2qq$ solutiones diversas praebent.

11. Constant methodi, quarum beneficio ex una solutione inventa aliae erui possunt; verum eae ad calculos nimium intricatos deducunt. Ita reperire licet

$$x = q(pp - qq)(3pp - qq)$$
$$y = (pp + qq)(p(pp + qq) \mp q(3pp + qq))$$

convenientes vero valores pro t et u § 2 suppeditat.

Solutio I. In hac solutione ratio numerorum x et y est $\frac{x}{y} = \frac{4}{3} \cdot \frac{pp - qq}{2pq}$; tum vero ratio $\frac{t}{u} = \frac{3xx + 4yy}{xx}$; unde solutiones simpliciores sunt:

1)	$x = 5$,	$y = 2$,	$t = 91$,	$u = 25$
2)	$x = 7$,	$y = 5$,	$t = 247$,	$u = 49$
3)	$x = 5$,	$y = 9$,	$t = 399$,	$u = 25$
4)	$x = 3$,	$y = 10$,	$t = 427$,	$u = 9$
5)	$x = 11$,	$y = 14$,	$t = 1147$,	$u = 121$
6)	$x = 15$,	$y = 7$,	$t = 871$,	$u = 225$
7)	$x = 16$,	$y = 5$,	$t = 217$,	$u = 64$
8)	$x = 16$,	$y = 9$,	$t = 273$,	$u = 64$
9)	$x = 7$,	$y = 18$,	$t = 1443$,	$u = 49$
10)	$x = 13$,	$y = 20$,	$t = 2107$,	$u = 169$.

Solutio II. Hic ratio numerorum x et y est $\frac{x}{y} = \frac{p(p + 2q)}{q(q + 2p)}$, numerorum t et u vero

$$\frac{t}{u} = \frac{p(q + 2p)(pp + 2pq + 3qq)}{q(p + 2q)(qq + 2pq + 3pp)}.$$

Si numeros x et y ut datos spectemus, ob

$$ppy + 2pqy = qqx + 2pqx,$$

reperitur

$$\frac{p}{q} = \frac{x - y + \sqrt{(xx - xy + yy)}}{y},$$

unde numerorum x et y character in hoc consistit, ut $xx - xy + yy$ sit quadratum; cujusmodi numeri cum facile inveniantur, sit $xx - xy + yy = zz$; eritque

$$\frac{p}{q} = \frac{x - y + z}{y} = \frac{x}{y - x + z}; \quad \text{seu} \quad \frac{p}{q} = \frac{z - y}{x - z};$$

hinc fit

$$\frac{p + 2q}{q + 2p} = \frac{2x - y - z}{z - 2y + x} = \frac{z + y}{z + x} \quad \text{et} \quad \frac{p(q + 2p)}{q(p + 2q)} = \frac{(z - y)(z + x - 2y)}{(z - x)(z + y - 2x)}$$

ut

$$(z - y)(z + x - 2y) = (z + x - y)(2z - x - y) \quad (z - x)(z + y - 2x) = (z + y - x)(2z - x - y)$$

unde $\frac{p(q + 2p)}{q(p + 2q)} = \frac{z + x - y}{z + y - x}$.

Deinde est

$$\frac{pp + 2pq + 3qq}{qq + 2pq + 3pp} = \frac{(x - y)^2 + 2(z - x)^2}{(x - y)^2 + 2(z - y)^2} = \frac{2z + y - x}{2z + x - y};$$

hincque tandem elicitur

$$\frac{t}{u} = \frac{(z+x-y)(2z-x+y)}{(z+y-x)(2z+x-y)}.$$

Sicque pro x et y ejusmodi numeris inventis, ut sit rationaliter $\sqrt{(xx-xy+yy)} = z$, capiatur:

$$t = (z+x-y)(2z-x+y) = xx+yy+(x-y)z$$
$$u = (z+y-x)(2z-y+x) = xx+yy-(x-y)z.$$

Hinc obtinetur

$$ttxx + uuyy = (xx+yy)(xx-2xy+yy+(x+y)z)^2$$
$$uuxx + ttyy = (xx+yy)(xx-2xy+yy-(x+y)z)^2,$$

vel etiam hoc modo

$$ttxx + uuyy = \tfrac{1}{4}(xx+yy)(x+y+z)^2(4z-x-y)^2$$
$$uuxx + ttyy = \tfrac{1}{4}(xx+yy)(x+y-z)^2(4z+x+y)^2.$$

Num autem quo facilius valores pro x et y idoneos reperiamus, spectemus x ut datum, ac ponamus $z = y - v$ eritque

$$xx - xy = -2yv + vv \quad \text{et} \quad y = \frac{xx-vv}{-2v+x} = \frac{vv-xx}{2v-x};$$

ubi pro quovis valore ipsius x assumto casus integri pro y sunt eruendi: notandum vero est, pro x numerum impariter parem assumi non posse, quia y quoque fieret par:

x	y	z	t	u
3	− 5	7	45	11
3	+ 8	7	19	54
5	+ 8	7	34	55
5	− 16	19	340	59
5	+ 21	19	81	385
7	− 8	13	154	41
7	+ 15	13	85	189
7	− 33	37	1309	171
7	+ 40	37	214	1435
8	+ 15	13	99	190
9	− 56	61	3591	374
9	+ 65	61	445	3861
11	− 24	31	891	194
11	+ 35	31	301	1045
11	− 85	91	8041	695
11	+ 96	91	801	8536
13	− 35	43	1729	335
13	+ 48	43	484	1989
13	− 120	127	15730	1161
13	+ 133	127	1309	16549

Problema 2. Invenire duo quadratorum paria xx, yy et tt, uu, ut
$$(ttxx + uuyy)(uuxx + ttyy)$$
sit numerus quadratus.

Solutio. Hoc problema eandem sortitur solutionem, quod praecedens, idemque quaterni numeri pro x, y, t, u inventi satisfaciunt. Inde ergo solutio simplicissima est
$$x = 3, \quad y = 5, \quad t = 11, \quad u = 45,$$
ex qua fit
$$ttxx + uuyy = 34.9.169, \quad uuxx + ttyy = 34.625$$
ideoque
$$(ttxx + uuyy)(uuxx + ttyy) = 34^2.39^2.25^2.$$
Ceterum haec solutio non solum ob eam causam tantum est particularis, ob quam talis erat, sed etiam hoc problema infinitas solutiones admittere videtur, quae praecedenti non conveniant. Fieri enim potest, ut haec formula
$$(ttxx + uuyy)(uuxx + ttyy)$$
fit quadratum, etiamsi neutra praecedentium
$$(xx + yy)(ttxx + uuyy) \quad \text{et} \quad (xx + yy)(uuxx + ttyy)$$
fuerit quadratum, cujus rei unicum exemplum dedisse sufficiat:
$$x = 973, \quad y = 263, \quad t = 973, \quad u = 1841$$
est enim
$$uuxx + ttyy = 2.25.263^2.973^2 \text{ quadratum duplicatum}$$
$$ttxx + uuyy = 2.25.141793^2 \quad \text{quadratum duplicatum.}$$
En adhuc aliam solutionem latius patentem
$$x = 3n^4 + 6mmnn - m^4, \quad t = mx$$
$$y = 3m^4 + 6mmnn - n^4, \quad u = ny,$$
cujus inventionis ratio facile intelligitur, posito enim $t = mx$ et $u = ny$ fit
$$ttxx + uuyy = mmx^4 + nny^4 \quad \text{et} \quad uuxx + ttyy = xxyy(mm + nn)$$
sicque ad quadratum reducenda est haec formula
$$(mm + nn)(mmx^4 + nny^4),$$
quae facto $x = v + z$ et $y = v - z$ ad istam solutionem perducit: hinc autem praecedentes solutiones non obtinentur.

Problema 3. Invenire duo quadratorum paria xx, yy et tt, uu, ut tam hic numerus $ttxx + uuyy$, quam iste $ttyy + uuxx$ fiat quadratus.

Solutio. Ex modo tradita solutione problematis praecedentis solutio hujus facile adornatur, pro m et n ejusmodi numeris sumendis, ut $mm + nn$ fiat quadratum. Sic si fiat $m = 4$ et $n = 3$ reperitur
$$x = 851, \quad t = 3404$$
$$y = 1551, \quad u = 3653.$$

At ex problemate primo multo concinniores solutiones impetrantur, quibus adeo praeter binas praescriptas conditiones et haec tertia adimpletur, ut $xx + yy$ fiat etiam quadratum. At solutio secunda primi problematis unum praebet casum, quo $xx + yy$ fit quadratum, scilicet

$$x = 8, \quad y = 15, \quad t = 99, \quad u = 190$$

unde fit

$$xx + yy = 17^2$$
$$ttxx + uuyy = 2^2 . 3^2 . 17^2 . 29^2$$
$$ttyy + uuxx = 5^2 . 5^2 . 5^2 . 17^2 .$$

Si insuper addita fuisset haec conditio, ut etiam $xx - xy + yy$ foret quadratum, eadem solutio negotium conficeret. Hujusmodi autem solutiones elicentur quaerendis numeris x et y, ut haec expressio

$$x^4 - x^3y + 2xxyy - xy^3 + y^4 \text{ fiat quadratum,}$$

ad quos porro ut ante numeros t et u investigari oportet.

Occasionem hoc problema Diophanteum tractandi praebuit problema geometricum a Schotenio propositum, quo datis in triangulo basi, perpendiculo et ratione laterum, ipsa latera quaeruntur. Problema hoc geminam admittit solutionem, quarum utraque ut praebeat latera rationaliter expressa, negotium ad problema istud Diophanteum perducitur. Si enim basis trianguli ponatur $= a$, perpendiculum $= b$, et laterum ratio $m:n$, vocatis ipsis lateribus mz et nz, primo necesse est a et b ita exprimi

$$a = (mm - nn)(xx + yy) \quad \text{et} \quad b = 2mnxy,$$

tum vero pro z haec duplex expressio reperitur:

$$z = \sqrt{(xx + yy)((m - n)^2 xx + (m + n)^2 yy)}$$
$$\text{et} \quad z = \sqrt{(xx + yy)((m + n)^2 xx + (m - n)^2 yy)},$$

quae ut ambae fiant rationales facto $m + n = t$, $m - n = u$, nascitur nostrum problema Diophanteum. Cujus ergo casus simplicissimus erit sumto

$$x = 3, \quad y = 5, \quad t = 45 \quad \text{et} \quad u = 11,$$

unde haec nascuntur data:

ratio laterum $m : n = 28 : 17$,
basis trianguli $a = 33$, et perpendiculum $b = 28$,

unde reperiuntur ipsa latera:

$$\text{vel} \quad mz = \frac{140}{3} \quad \text{et} \quad nz = \frac{85}{3},$$
$$\text{vel} \quad mz = \frac{364}{5} \quad \text{et} \quad nz = \frac{221}{5},$$

sive in integris sumta

basis $a = 495$ et perpendiculum $b = 420$

obtinebuntur latera rationem $28 : 17$ tenentia

$$\text{vel} \quad mz = 700 \quad \text{et} \quad nz = 425$$
$$\text{vel} \quad mz = 1092 \quad \text{et} \quad nz = 663.$$

XXXII.

Problematis cujusdam Diophantei evolutio.

(N. Comment. XVII. 1772. p. 24. Exhib. 1772 Jan. 13.)

1. Cum olim istud problema Diophanteum tractassem, quo quaerebantur tres numeri, quo 1) summa 2) summa productorum ex binis et 3) productum omnium sint numeri quadrati(*), solutio tantis difficultatibus implicata videbatur, ut hujus generis problemata adhuc difficiliora vix aggredi essem ausus. Multo autem difficilius esse problema, cujus enodationem hic suspicio, nemo dubitabit, qui ejus solutionem tentare voluerit. Problema autem hoc ita se habet:

Invenire quatuor numeros ejus indolis, ut 1) *summa singulorum*, 2) *summa factorum ex binis*, 3) *summa factorum ex ternis et* 4) *productum omnium sint numeri quadrati.*

Vel quod eodem redit

Invenire aequationem biquadraticam hujus formae: $x^4 - Ax^3 + Bx^2 - Cx + D = 0$, *quae omnes suas radices habeat rationales, et cujus insuper singuli coefficientes* A, B, C, D *sint numeri quadrati.*

2. Non dubito fore plerosque, qui mirabuntur, me in hujusmodi quaestionibus evolvendis, quas nunc quidem summi Geometrae aversari videntur, operam consumere; verum equidem fateri cogor, me ex hujusmodi investigationibus tantundem fere voluptatis capere, quam ex profundissimis Geometriae sublimioris speculationibus. Ac si plurimum studii et laboris impendi in quaestionibus gravioribus evolvendis, hujusmodi variatio argumenti quandam mihi haud ingratam recreationem afferre solet. Ceterum analysis sublimior tantum debet methodo Diophanteae, ut nefas videatur eam penitus repudiare.

3. Problema igitur propositum aggressurus, primum observo, solutionem ejus generalem frustra tentari; postquam enim pluribus modis calculum instituissem, ac semper in formulas nullo pacto extricabiles incidissem, agnovi vix quicquam praestari posse, nisi vires nostras in solutionem quandam particularem intendamus. Sequenti ergo modo quatuor numeros quaesitos constituo:

$$Mab, \quad Mbc, \quad Mcd, \quad Mda,$$

ubi etsi quinque litterae sunt inductae, tamen haec positio ista limitatione restringitur, ut productum primi in tertium aequale sit producto secundi in quartum: quae restrictio utique in se non est necessaria, vixque dubitare licet, quin etiam ejusmodi quaterni numeri quaesito satisfaciant, in quibus haec conditio locum non habeat; verum equidem nullam adhuc viam detegere valui, qua hujusmodi solutiones elicere liceret.

4. Hac igitur numerorum quaesitorum forma constituta, quatuor conditiones praescriptae sequentes aequationes suppeditant:

(*) Vide supra pag. 239 sqq.

$$\text{I.}\quad M(ab + bc + cd + da) = \square,$$
$$\text{II.}\quad M^2(abbc + bccd + cdda + daab + 2abcd) = \square,$$
$$\text{III.}\quad M^3(abbccd + abccdd + aabcdd + aabbcd) = \square,$$
$$\text{IV.}\quad M^4 aabbccdd = \square,$$

ubi postrema conditio jam sponte impletur, neque vero hinc concludere licet, limitationem supra inductam esse necessariam; cum eadem conditio aeque obtineretur, si quis quatuor numerorum insuper per numerum quadratum quemcunque multiplicaretur, quo pacto solutio ab omni restrictione liberaretur, sed tum reliquae aequationes nullo modo resolvi possent.

5. Restrictio autem adhibita hoc commodi nobis largitur, ut tertia aequatio hanc formam induat

$$M^3 abcd(ab + bc + cd + da) = \square$$

unde cum ob primam jam quadratum esse debeat haec forma

$$M(ab + bc + cd + da),$$

necesse est, ut hoc productum $abcd$ quadrato aequetur. Praeterea autem ut tam primae quam tertiae conditioni satisfiat, capi oportet

$$M = ab + bc + cd + da,$$

vel si haec summa factorem habeat quadratum puta ff, sufficiet sumi

$$M = \frac{ab + bc + cd + da}{ff},$$

siquidem per se manifestum est, solutionem semper ad numeros integros reduci posse.

6. Hinc jam ratio est perspicua, cur initio quatuor quaesitis numeris factorem communem M tribuerim; eo igitur rite definito, ut sit

$$M = ab + bc + cd + da, \quad \text{vel} \quad M = \frac{ab + bc + cd + da}{ff}$$

duae tantum supersunt conditiones, quas impleri oportet; alteram scilicet modo elicui, qua esse debet

$$abcd = \square;$$

alteram aequatio secunda suppeditat, quae postulat ob factorem M^2 jam quadratum, ut sit

$$abbc + bccd + acdd + aabd + 2abcd = \square,$$

quae in hanc formam redigitur:

$$(aa + cc)bd + ac(bb + dd) + 2abcd = \square,$$

seu
$$bd(aa + cc) + (b + d)^2 ac = \square.$$

7. Tota ergo quaestio ad inventionem hujusmodi quatuor numerorum a, b, c, d est perducta, ut binis modo memoratis conditionibus satisfiat; ubi notari convenit, inter binos numeros a et c similem rationem intercedere atque inter binos b et d; atque totum negotium a sola ratione tam inter a et c quam inter b et d pendere. Quare ut pro quavis solutione minimos numeros obtineamus, tam numeros a et c quam b et d primos inter se statui oportet. Si enim communem haberent divisorem, eo sublato conditioni utrique aeque satisfieret.

8. Quia evolutio posterioris aequationis praecipuas difficultates involvit, ab ea inchoandum esse arbitror, ac primo quidem observo, etiamsi ea duas rationes $a:c$ et $b:d$ contineat, neutram

tamen arbitrio nostro relinqui; unde imprimis inquirendum est, cujusmodi rationes pro alterutra accipi debeant, ut forma nostra quadratum reddi possit. Quod quo facilius perspiciatur, consideremus casum, quo loco alterius rationis ratio dupla poneretur, sit ergo $b:d = 2:1$, et haec forma $2aa + 2cc + 9ac$ quadratum reddi deberet; quod autem nunquam fieri posse facile intelligitur. Posito enim $a = p + q$ et $c = p - q$, prodit haec forma $13pp - 5qq$, quae nullo modo unquam quadratum exhibere potest: idem evenit si poneretur $b:d = 3:1$; unde patet nonnisi certas rationum species pro alterutra rationum $a:c$ et $b:d$ assumi posse; reliquas vero omnes ab hac investigatione excludi.

9. Statim autem patet inter rationes huic scopo accommodatas primum locum obtinere rationes quadraticas; sit igitur $b:d = pp:qq$, et formula nostra

$$ppqq\,(aa + cc) + ac\,(pp + qq)^2$$

aequetur huic quadrato $ppqqaa + \frac{2m}{n}pqac + \frac{mm}{nn}cc$, unde fit

$$nn\,(pp + qq)^2 a + nnppqqc = 2mnpqa + mmc$$

ideoque

$$\frac{a}{c} = \frac{mm - nnppqq}{nn\,(pp + qq)^2 - 2mnpq},$$

vel sit $m = \pm kpq$, ut habeamus has formulas satisfacientes

$$\frac{b}{d} = \frac{pp}{qq} \quad \text{et} \quad \frac{a}{c} = \frac{(kk - nn)\,ppqq}{nn\,(pp + qq)^2 \pm 2knppqq} \quad \text{existente } k > n.$$

10. Evolvamus casus simpliciores numerorum k et n, et habebimus aequationis nostrae sequentes resolutiones

si fuerit $\frac{b}{d} = \frac{pp}{qq}$, erit

I. $\frac{a}{c} = \frac{3ppqq}{(pp + qq)^2 \pm 4ppqq}$, II. $\frac{a}{c} = \frac{8ppqq}{(pp + qq)^2 \pm 6ppqq}$,

III. $\frac{a}{c} = \frac{5ppqq}{4\,(pp + qq)^2 \pm 12ppqq}$, IV. $\frac{a}{c} = \frac{15ppqq}{(pp + qq)^2 \pm 8ppqq}$,

V. $\frac{a}{c} = \frac{7ppqq}{9(pp + qq)^2 \pm 24ppqq}$, VI. $\frac{a}{c} = \frac{24ppqq}{(pp + qq)^2 \pm 10ppqq}$,

VII. $\frac{a}{c} = \frac{21ppqq}{4(pp + qq)^2 \pm 20ppqq}$, VIII. $\frac{a}{c} = \frac{16ppqq}{9\,(pp + qq)^2 \pm 30ppqq}$,

IX. $\frac{a}{c} = \frac{9ppqq}{16\,(pp + qq)^2 + 40ppqq}$, etc.

11. Si jam pro litteris k, n, p, q ejusmodi valores inveniri possent, ut productum ac seu haec expressio

$$n\,(kk - nn)\,(n\,(pp + qq)^2 \pm 2kppqq)$$

fieret numerus quadratus, haberetur solutio problematis propositi, siquidem tum ob $bd = ppqq$ etiam formula $abcd$ foret quadratum. Verum haec investigatio nimis est molesta, quam ut eam suscipi conveniat; ac si forte succederet, ad maximos numeros certe perduceret. Quare consultum erit etiam alias rationes pro $\frac{b}{d}$ contemplari, quae quidem alteri conditioni scilicet

$$bd\,(aa + cc) + ac\,(b + d)^2 = \square$$

convenire queant. At ob similem rationem fractionum $\frac{b}{d}$ et $\frac{a}{c}$ omnes valores hic pro $\frac{a}{c}$ eruti etiam vicissim pro $\frac{b}{d}$ assumi poterunt, unde denuo novae hujus generis fractiones elicientur.

12. In genere quidem hic labor nimis foret taediosus, unde casus primo simpliciores evolvam:

$$\text{si } \frac{b}{d}=\frac{1}{1}, \text{ erit } \frac{a}{c}=\frac{3}{8}, -\frac{4}{1}, \frac{4}{5}, \frac{5}{28}, -\frac{15}{4}, \frac{7}{12}, \frac{7}{60}, \frac{8}{33};$$

$$\text{si } \frac{b}{d}=\frac{4}{1}, \text{ erit } \frac{a}{c}=\frac{3}{4}, \frac{12}{41}, \frac{32}{1}, \frac{32}{49}, \frac{5}{13}, \frac{5}{37}, -\frac{60}{7}, \frac{20}{19};$$

$$\text{si } \frac{b}{d}=\frac{9}{1}, \text{ erit } \frac{a}{c}=\frac{27}{64}, \frac{27}{136}, \frac{36}{23}, \frac{36}{77}, \frac{45}{292}, \frac{108}{5};$$

$$\text{si } \frac{b}{d}=\frac{9}{4}, \text{ erit } \frac{a}{c}=\frac{108}{25}, \frac{45}{61}, \frac{28}{73}, \frac{64}{49}, \frac{64}{289};$$

En ergo hic praeter expectationem duos casus, quibus pro a et c numeri quadrati prodierunt; unde cum etiam b et d sint numeri quadrati, duas jam sumus adepti problematis nostri solutiones.

13. En ergo duas problematis nostri solutiones; quarum prima ob $a=64$, $b=9$, $c=49$ et $d=4$ praebet:

$$M=576+441+196+256=1469$$

sicque quatuor numeri quaesiti sunt

$$\text{I. } 1469.196, \quad \text{II. } 1469.256, \quad \text{III. } 1469.441, \quad \text{IV. } 1469.576.$$

Altera ob $a=64$, $b=9$, $c=289$, $d=4$, dat

$$M=576+2601+1156+256=4589$$

unde alii quatuor numeri problemati satisfacientes sunt

$$\text{I. } 4589.256, \quad \text{II. } 4589.576, \quad \text{III. } 4589.1156, \quad \text{IV. } 4589.2601.$$

Has autem solutiones haud facile ex formula § 11 data derivare licuisset, etiamsi in ea contineantur.

14. Cum autem singulae fractiones pro $\frac{a}{c}$ inventae etiam pro $\frac{b}{d}$ usurpari queant, evolvamus simpliciores, quae sunt:

$$\frac{4}{3}, \frac{5}{4}, \frac{8}{3}, \frac{12}{7}, \frac{13}{5}, \frac{20}{19}, \frac{28}{5}, \frac{32}{1}, \frac{33}{8} \text{ etc}$$

Sit igitur primo $\frac{b}{d}=\frac{4}{3}$ et habebitur

$$12aa+12cc+49ac=\square,$$

cui satisfacit $\frac{a}{c}=4$, ponatur ergo $\frac{a}{c}=4+x$

$$\begin{array}{l} 192+\ 96x+12xx \\ +\ 12 \\ 196+\ 49x \\ \hline 400+145x+12xx=\square=(20+xy)^2, \end{array}$$

ergo

$$145+\ 12x=40y+xyy \quad \text{et} \quad x=\frac{145-40y}{yy-12}$$

hincque $\frac{a}{c} = \frac{4yy - 40y + 97}{yy - 12}$, seu posito $y = \frac{m}{n}$

$$\frac{a}{c} = \frac{4mm - 40mn + 97nn}{mm - 12nn}$$

unde sequentes novae fractiones idoneae simpliciores colliguntur

$$\frac{a}{c} = \frac{24}{1}, \ \frac{37}{13}, \ \frac{121}{24}.$$

15. Statuatur simili modo $\frac{b}{d} = \frac{5}{4}$ fietque

$$20aa + 20cc + 81ac = \square,$$

cui satisfacit $\frac{a}{c} = 1$, sit ergo $\frac{a}{c} = 1 + x$

$$\begin{array}{l} 20 + \ 40x + 20xx \\ 20 \\ 81 + \ 81x \\ \hline 121 + 121x + 20xx = \square = (11 + xy)^2, \end{array}$$

ergo

$$121 + 20x = 22y + xyy \quad \text{et} \quad x = \frac{121 - 22y}{yy - 20} \quad \text{et} \quad \frac{a}{c} = \frac{yy - 22y + 101}{yy - 20} = \frac{mm \pm 22mn + 101nn}{mm - 20nn}$$

unde elicitur $\frac{a}{c} = \frac{16}{5}$, ita ut sit $abcd$ quadratum.

16. Haec solutio nobis largitur quatuor numeros multo minores problemati satisfacientes. Cum enim habeamus:

$$a = 16, \quad b = 5, \quad c = 5, \quad d = 4,$$

erit factor communis

$$M = \frac{80 + 25 + 20 + 64}{ff} = \frac{189}{ff},$$

unde sumto $f = 3$, erit $M = 21$, et quatuor numeri problema solventes erunt

I. $21 \cdot 20$, II. $21 \cdot 25$, III. $21 \cdot 64$ et IV. $21 \cdot 80$.

quorum summa singulorum est $= 9 \cdot 21^2$,

summa productorum ex binis $= 110^2 \cdot 21^2$,

summa productorum ex ternis $= 4800^2 \cdot 21^4$,

productorum omnium $= 1600^2 \cdot 21^4$,

ita ut hujus aequationis biquadraticae

$$x^4 - 9 \cdot 21^2 \cdot x^3 + 110^2 \cdot 21^2 \cdot xx - 4800^2 \cdot 21^4 \cdot x + 1600^2 \cdot 21^4 = 0,$$

radices sint $21 \cdot 20$, $21 \cdot 25$, $21 \cdot 64$, $21 \cdot 80$.

17. Ex cognita autem una solutione, certa methodo aliae imo infinitae elici possunt; quod quo facilius ostendam, hac postrema solutione utar, qua posito $\frac{b}{d} = \frac{5}{4}$ invenimus in genere $\frac{a}{c} = \frac{yy - 22y + 101}{yy - 20}$, unde ut $abcd$ fiat quadratum, reddi oportet hanc formam:

$$5(yy - 20)(yy - 22y + 101) = \square$$

id quod evenit sumto $y = 5$. Statuatur ergo $y = z + 5$ et habebitur:

$$5(zz + 10z + 5)(zz - 12z + 16) = \square,$$

$$\text{seu} \quad 400 + 500z - 495zz - 10z^3 + 5z^4 = \square,$$

cui etiam satisfacit $z = 1$ et $y = 6$, unde autem eadem solutio resultat.

18. Ut aliam solutionem eliciamus, fingamus radicem quadratam hujus formae $20 + \frac{25}{2}z - \frac{521}{32}zz$, cujus quadratum

$$400 + 500z - 495zz - \frac{25.521}{32}z^3 + \frac{521^2}{32^2}z^4$$

illi formae aequatum praebet

$$\left(\frac{521^2}{32^2} - 5\right)z = \frac{25.521}{32} - 10,$$

$$\text{seu} \quad z = \frac{32.12705}{266331} = \frac{32.1155}{24211} = \frac{32.105}{2201}$$

ideoque $z = \frac{3360}{2201}$ et $y = \frac{14365}{2201}$, unde pro a et c numeri enormes resultant, quos evolvere operae non est pretium.

19. Ut autem plures solutiones derivare liceat, ob casum cognitum $z = 1$, ponamus $z = \frac{1}{1+v}$, et prodibit haec forma ad quadratum redigenda

$$\begin{array}{l} 400 + 1600v + 2400v^2 + 1600v^3 + 400v^4 \\ + 500 + 1500v + 1500v^2 + \ \ 500v^3 \\ - 495 - \ \ 990v + \ \ 495v^2 \\ - \ \ 10 - \ \ \ 10v \\ + \ \ \ 5 \\ \hline \end{array}$$

$$\text{seu} \quad 400 + 2100v + 3405v^2 + 2100v^3 + 400v^4 = \square,$$

cujus radix posita $= 20 + \frac{105}{2}v - 20vv$ dat

$$4205 - \frac{105^2}{4} + 4200v = 0,$$

$$\text{seu} \quad v = -\frac{1159}{3360} \quad \text{et} \quad 1 + v = \frac{2201}{3360} \quad \text{ut ante.}$$

Ob formam reciprocam erit etiam

$$v = -\frac{3360}{1159}, \quad 1 + v = -\frac{2201}{1159} \quad \text{et} \quad z = -\frac{1159}{2201}, \quad \text{hincque} \quad y = \frac{9846}{2201}$$

unde autem non alia solutio obtinetur.

20. Quanquam autem hoc modo ex qualibet solutione aliae innumerae deduci possunt; tamen quia in primas casu quasi fortuito incidimus, methodus adhuc certa desideratur, quae ad hujus problematis solutionem perducat; cujus inventio in analysi Diophantea utique maximi foret momenti. Verum antequam talem methodum expectare liceat, necesse videtur, ut natura hujus formae

$$ac(xx + yy) + (a + c)^2 xy$$

ad quadratum reducendae accuratius investigetur, et rationes pro $a:c$ assumendae, quibus resolutio succedit, explorentur; unde hanc quaestionem perscrutandam propono:

Invenire omnes valores idoneos pro ratione a : c *substituendos, ut haec expressio:*

$$ac(xx + yy) + xy(aa + cc) + 2acxy$$

quadrato aequalis reddi possit.

21. Ex superioribus jam satis liquet, rationem $a:c$ neutiquam pro lubitu accipi posse, sed eam certis conditionibus esse adstrictam, quas potissimum determinari oportet.

Ad has conditiones explorandas statuamus:

$$ac(xx+yy)+xy(aa+cc)+2acxy=zz,$$

quam aequationem in sequentes formas transfundere licet:

$$\text{I.}\quad (aa+cc)(xx+yy)=(a+c)^2(x+y)^2-2zz,$$

$$\text{II.}\quad (aa+4ac+cc)(xx+4xy+yy)=6zz+(a-c)^2(x-y)^2,$$

$$\text{III.}\quad (aa+cc)(xx+4xy+yy)=2zz+(a-c)^2(x+y)^2,$$

$$\text{IV.}\quad (aa+4ac+cc)(xx+yy)=2zz+(a+c)^2(x-y)^2.$$

22. Cum jam ex prima forma intelligamus, formulam $aa+cc$ factorem esse numeri hujus formae $tt-2zz$, qui, uti constat, alios non admittit divisores, nisi qui ipsi sint vel hujus formae $AA-2BB$, vel hujus $2AA-BB$, sequitur numerum $aa+cc$ in alterutra harum formarum contineri debere. Ex tertia autem forma intelligitur, eundem numerum $aa+cc$, cum sit divisor formae $2zz+tt$, etiam in forma $2AA+BB$ contineri debere. Jam vero numeri formae $2AA-BB$, vel $AA-2BB$ praeter binarium alios non habent divisores primos, nisi qui in forma $8n\pm 1$ contineantur, et numeri formae $2AA+BB$ alios non habent divisores primos praeter binarium, nisi qui vel in hac forma $8n+1$, vel $8n+3$ contineantur. Ex quo concluditur haec conditio, ut numerus $aa+cc$ alios praeter binarium non habeat divisores primos, nisi qui sint formae $8n+1$.

23. Simili modo cum altera formula $aa+4ac+cc$ sit divisor formae $6zz+tt$, quae alios divisores praeter 2 et 3 non admittit primos, nisi qui in aliqua harum formularum:

$$24n+1,\quad 24n+5,\quad 24n+7,\quad 24n+11$$

contineantur; tum vero quia eadem formula $aa+4ac+cc$ etiam est divisor formae $2zz+tt$, ea praeter 2 alios non admittit divisores primos, nisi qui in alterutra harum formarum $8n+1$, vel $8n+3$ contineantur. Ex quibus conjunctis sequitur numerum $aa+4ac+cc$ praeter 2 et 3 alios divisores primos habere non posse, nisi qui contineantur vel in hac formula $24n+1$, vel hac $24n+11$.

24. Hinc e valoribus rationis $a:c$ primum omnes ii excluduntur, quibus numerus $aa+cc$ haberet divisorem primum formae $8n+5$, siquidem reliquae formae ineptae $8n+3$ et $8n+7$ sponte excluduntur, propterea quod summa duorum quadratorum $aa+cc$ per tales numeros nunquam divisibilis existit. Deinde etiam ii valores rationis $a:c$ excluduntur, quibus numerus $aa+4ac+cc$ qui per se praeter 2 et 3 alios habere nequit divisores, nisi qui sint hujus formae $12n+1$, vel hujus formae $12n+11$, haberet divisorem vel hujus formae $24n+13$, vel hujus $24n+23$. Quocirca ex rationibus pro $a:c$ adhibendis primo expungi debent omnes eae, quibus numerus $aa+cc$, dividi potest per numerum primum formae $8n+5$, deinde etiam eae, quibus numerus $aa+4ac+cc$ admitteret divisorem formae $24n+13$, vel $24n+23$.

25. Quando autem ratio $a:c$ ita est comparata, ut numerus $aa+cc$ nullum habeat divisorem formae $8n+5$; tum vicissim certum est, eundem numerum tam in hac forma $2AA-BB$ quam hac $2AA+BB$ contineri. Ac si quoque numerus $aa+4ac+cc$ nullum habeat divisorem formae $24n+13$, vel $24n+23$, tum perinde certum est, eundem numerum tam in hac forma $2AA+BB$ quam ista $6AA+BB$ contineri. Hac duplici regula observata facili negotio omnes rationes, quas loco $a:c$ assumi non licet, excluduntur.

26. Facta autem hac exclusione, pro fractione $\frac{a}{c}$ sequentes valores sunt relicti:

$$\frac{1}{1}, \frac{4}{1}, \frac{4}{3}, \frac{5}{4}, \frac{8}{3}, \frac{8}{7}, \frac{9}{1}, \frac{9}{4}, \frac{11}{4}, \frac{12}{5}, \frac{12}{7}, \frac{13}{5}, \frac{13}{12},$$

$$\frac{15}{7}, \frac{15}{8}, \frac{16}{1}, \frac{16}{5}, \frac{16}{9}, \frac{16}{13}, \frac{17}{12}, \frac{19}{8}, \frac{19}{11}, \frac{20}{1}, \frac{20}{3}, \frac{20}{7}, \frac{20}{11},$$

$$\frac{20}{13}, \frac{20}{19}, \frac{21}{5}, \frac{21}{20}, \frac{23}{8}, \frac{24}{1}, \frac{24}{5}, \frac{24}{7}, \frac{24}{11}, \frac{24}{19}, \frac{25}{1}, \frac{25}{4}, \frac{25}{9},$$

$$\frac{25}{12}, \frac{25}{16}, \frac{25}{17}, \frac{27}{11}, \frac{27}{20}, \frac{28}{5}, \frac{28}{13}, \frac{28}{15}, \frac{28}{25}, \frac{29}{3},$$

ubi observari convenit, reliquas rationes omnes frustra adhibitum iri: num autem hae omnes post exclusiones expositas relictae succedant, quaestio est maximi momenti, quae vix decidi posse videtur.

27. Hic prima ratio, in praecedentibus nondum inventa est $\frac{8}{7}$, quae igitur an solutionem quaestionis admittat, videamus. Fieri nempe oportet:

$$56\,(xx + yy) + 225\,xy = \Box.$$

Ponatur $x = p + q$ et $y = p - q$, ut prodeat haec forma:

$$337\,pp - 113\,qq = \Box,$$

quod an fieri possit, facilius exploratur, quam ex forma praecedente; satisfaciunt autem hi valores minimi $p = 3$ et $q = 4$, unde colligitur $x = 7$ et $y = -1$, seu $\frac{x}{y} = -7$, statuatur ergo $\frac{x}{y} = \frac{-7+v}{1}$, et prodit:

$$1225 - 559\,v + 56\,vv = \Box,$$

unde colligitur

$$v = \frac{70t - 559}{tt - 56} \quad \text{et} \quad \frac{x}{y} = \frac{-7tt + 70t - 167}{tt - 56}, \quad \text{seu} \quad \frac{x}{y} = \frac{7tt - 70t + 167}{56 - tt} = \frac{7mm - 14mn - nn}{20nn + 12mn - mm}.$$

28. Cum deinde etiam alios plures casus examinassem, inveni negotium semper succedere; ex quo asseverare vix dubito, omnes istas fractiones, post binas exclusiones ante memoratas relictas, semper ita esse comparatas, ut loco rationis $a:c$ positae aequationem

$$ac\,(xx + yy) + (a + c)^2\,xy = \Box$$

resolubilem reddant. Nunc igitur omnino operae foret pretium in indolem harum fractionum accuratius inquirere, earumque verum characterem indagare, quo eae ab omnibus reliquis fractionibus distinguuntur. Primo quidem patet, in iis omnes fractiones hujus formae $\frac{pp}{qq}$ occurrere, quomodo autem reliquarum indoles sit comparata, altioris videtur indaginis.

29. Videamus autem, quomodo in genere numeri a et c comparati esse debeant, ut $aa + cc$ obtineat formam $AA - 2BB$. Posito autem

$$aa + cc = AA - 2BB, \quad \text{erit} \quad AA - aa = cc + 2BB,$$

ideoque tam $A + a$ quam $A - a$, utpote divisores formae $cc + 2BB$, ejusdem formae numeri esse debent; unde posito

$$A + a = pp + 2qq \quad \text{et} \quad A - a = rr + 2ss,$$

fit
$$A=\frac{pp+2qq+rr+2ss}{2} \quad \text{et} \quad a=\frac{pp+2qq-rr-2ss}{2}$$
et ob $cc+2BB=(pp+2qq)(rr+2ss)$, erit
$$c=2qs+pr \quad \text{et} \quad B=ps-qr.$$
Quocirca conditio praescripta impletur sumendo
$$a=pp-rr+2qq-2ss \quad \text{et} \quad c=2pr+4qs,$$
unde fit
$$aa+cc=(pp+rr)^2+4(qq+ss)^2+4(pp-rr)(qq-ss)+16pqrs,$$
quae forma non solum est
$$=(pp+rr+2qq+2ss)^2-2(2ps-2qr)^2,$$
sed etiam
$$=(pp+rr-2qq-2ss)^2+2(2pq+2rs)^2.$$
Unde tam in hac forma $AA-2BB$ quam ista $AA+2BB$ continetur.

30. Evolvamus simili modo alteram conditionem, quae postulat
$$aa+4ac+cc=AA+2BB,$$
et cum fiat
$$(a+2c)^2-3cc=AA+2BB, \quad \text{seu} \quad (a+2c)^2-AA=2BB+3cc$$
debet esse:
$$a+2c+A=2tt+3uu \quad \text{et} \quad a+2c-A=xx+yy,$$
ergo
$$a+2c=\frac{2tt+3uu+xx+yy}{2}.$$
Tum vero ob $2BB+3cc=(2tt+3uu)(xx+yy)$ fit
$$B=tx-3uy \quad \text{et} \quad c=ux+2ty,$$
ideoque
$$a=2tt-8ty+6yy+3uu-4ux+xx,$$
seu
$$a=2(t-y)(t-3y)+(u-x)(3u-x)$$
et
$$c=2ux+4ty.$$
Vel sit $t=y+v$ et $x=u-z$, ut fiat
$$a=2v(y-2v)+z(z+2u),$$
$$c=4y(y+v)+2u(u-z),$$
hocque modo simul alteri conditioni, qua esse debet $aa+4ac+cc=6AA+BB$, satisfit.

31. Quo igitur utrique conditioni satisfiat, necesse est, ut ambo numeri a et c simul in sequentibus binis formulis contineantur:
$$a=(p-r)(p+r)+2(q-s)(q+s), \quad c=2pr+4qs;$$
$$a=(u-x)(3u-x)+2(t-y)(t-3y), \quad c=2ux+4ty.$$
Nova ergo hinc nascitur quaestio: quomodo hae binae geminae formulae ad eundem valorem sint reducendae; ad quod necesse est, ut huic aequalitati satisfiat:
$$(ux+2ty)(pp-rr+2qq-2ss)=(pr+2qs)(3uu-4ux+xx+2tt-8ty+6yy)$$
quoniam totum negotium in ratione $a:c$ versatur.

Aliud problema Diophanteum.

Invenire quotcunque numeros, quorum quilibet in summam reliquorum multiplicatus producat numerum quadratum.

32. Sint numeri quaesiti p, q, r, s etc. eorumque summa $= S$: requiritur ergo, ut omnes hae formulae:

$$p(S-p),\quad q(S-q),\quad r(S-r),\quad s(S-s) \text{ etc.}$$

sint quadrata, quae cum sint similes, sufficit pro una posuisse $p(S-p) = ffpp$, unde fit $p = \frac{S}{1+ff}$. Quare numeri quaesiti erunt

$$\frac{S}{1+ff},\quad \frac{S}{1+gg},\quad \frac{S}{1+hh},\quad \frac{S}{1+kk} \text{ etc.}$$

dummodo eorum summa fiat $= S$; sicque problema huc redit, ut quaerantur numeri quotcunque f, g, h, k etc. ita comparati, ut fiat

$$\frac{1}{1+ff} + \frac{1}{1+gg} + \frac{1}{1+hh} + \frac{1}{1+kk} + \text{etc.} = 1.$$

33. Statuamus, quoniam hi numeri plerumque sunt fracti,

$$f = \frac{a}{\alpha},\quad g = \frac{b}{\beta},\quad h = \frac{c}{\gamma},\quad k = \frac{d}{\delta} \text{ etc.}$$

et quaestio huc redit, ut aliquot fractiones hujusmodi

$$\frac{\alpha\alpha}{aa+\alpha\alpha},\quad \frac{\beta\beta}{bb+\beta\beta},\quad \frac{\gamma\gamma}{cc+\gamma\gamma} \text{ etc.}$$

inveniantur, quorum summa unitati aequetur; ubi observo, quemlibet denominatorem esse summam duorum quadratorum. Quodsi ergo talis denominator sit numerus primus, ex eo duae tantum ejusmodi nascuntur fractiones, scilicet

$$\frac{aa}{aa+\alpha\alpha} \quad\text{et}\quad \frac{\alpha\alpha}{aa+\alpha\alpha},$$

quarum summa cum unitati aequetur, evidens est, ambas simul capi non posse, nisi quaestio de duobus numeris instituatur, quorum alter in alterum ductus praebeat quadratum. Tum enim ob

$$\frac{aa}{aa+\alpha\alpha} + \frac{\alpha\alpha}{aa+\alpha\alpha} = 1,$$

sumto S pro lubitu, numeri satisfacientes erunt Maa et $M\alpha\alpha$, qui propterea casus nullam habet difficultatem.

34. Quando autem plures duobus numeri sunt investigandi, qui problemati conveniant, necesse est, ut etiam casus, quibus denominatores sunt numeri compositi, evolvantur, siquidem inde plures fractiones hujus indolis formari possunt; quarum cum binae itidem unitati aequentur, sequenti modo eas repraesentabo:

Denominator $D = (aa+\alpha\alpha)(bb+\beta\beta)$

$$\frac{(ab-\alpha\beta)^2}{D} \quad\Big|\quad \frac{(a\beta+\alpha b)^2}{D}$$

$$\frac{(a\beta-\alpha b)^2}{D} \quad\Big|\quad \frac{(ab+\alpha\beta)^2}{D}.$$

Denominator $D = (aa + \alpha\alpha)(bb + \beta\beta)(cc + \gamma\gamma)$

$\frac{(\alpha\beta c + abc - ab\gamma + \alpha\beta\gamma)^2}{D}$	$\frac{(\alpha\beta\gamma + \alpha b\gamma + abc - \alpha\beta c)^2}{D}$
$\frac{(a\beta\gamma + ab\gamma - abc + a\beta c)^2}{D}$	$\frac{(a\beta c + \alpha bc + ab\gamma - \alpha\beta\gamma)^2}{D}$
$\frac{(abc + \alpha\beta c - \alpha\beta\gamma + \alpha b\gamma)^2}{D}$	$\frac{(ab \cdot + \alpha\beta\gamma + a\beta c - \alpha bc)^2}{D}$
$\frac{(ab\gamma + \alpha\beta\gamma - a\beta c + \alpha bc)^2}{D}$	$\frac{(abc + \alpha\beta c + a\beta\gamma - \alpha b\gamma)^2}{D}$.

35. Circa ordinem secundum annotasse juvabit, esse

$$\frac{(ab - \alpha\beta)^2}{D} + \frac{(a\beta - \alpha b)^2}{D} = 1 - \frac{4ab\alpha\beta}{D}$$

et
$$\frac{(ab - \alpha\beta)^2}{D} + \frac{(\alpha b + a\beta)^2}{D} = -1 + \frac{aabb + \alpha\alpha\beta\beta - aa\beta\beta - \alpha\alpha bb}{D}.$$

Deinde in ordine tertio, si quatuor partes prioris columnae invicem addantur, summa erit

$$2 - \frac{8(aa - \alpha\alpha)\, b\beta c\gamma}{(aa + \alpha\alpha)(bb + \beta\beta)(cc + \gamma\gamma)}.$$

Hinc non contemnenda subsidia peti poterunt pro quavis numerorum quaesitorum multitudine, dum, si solutio in genere tentaretur, insignes difficultates occurrerent. Quoniam igitur casus duorum numerorum per se est perspicuus, a casu trium exordiar, inde ad quatuor progressurus.

Casus trium numerorum.

36. Ponamus pro tribus numeris quaesitis has fractiones:

$$\frac{aa}{aa + \alpha\alpha}, \quad \frac{(ab - \alpha\beta)^2}{(aa + \alpha\alpha)(bb + \beta\beta)}, \quad \frac{(a\beta - \alpha b)^2}{(aa + \alpha\alpha)(bb + \beta\beta)},$$

quarum summa est

$$\frac{aa}{aa + \alpha\alpha} + 1 - \frac{4a\alpha b\beta}{(aa + \alpha\alpha)(bb + \beta\beta)} \quad \text{unitati aequanda,}$$

unde fit

$$aa(bb + \beta\beta) = 4a\alpha b\beta \quad \text{hincque} \quad \frac{a}{\alpha} = \frac{4b\beta}{bb + \beta\beta}.$$

Quare sumtis $a = 4b\beta$ et $\alpha = bb + \beta\beta$, numeri quaesiti ad integros perducti erunt:

$$aa(bb + \beta\beta), \quad (ab - \alpha\beta)^2, \quad (a\beta - \alpha b)^2.$$

Jam vero est

$$ab - \alpha\beta = 3bb\beta - \beta^3 = \beta(3bb - \beta\beta)$$
$$a\beta - \alpha b = 3b\beta\beta - b^3 = b(3\beta\beta - bb).$$

Consequenter habebimus has formulas

$$16bb\beta\beta(bb + \beta\beta), \quad \beta\beta(3bb - \beta\beta)^2, \quad bb(3\beta\beta - bb)^2,$$

quarum quaelibet in summam reliquarum ducta producit quadratum.

37. Evolvamus hinc solutiones simpliciores, ponendo numeros minores loco b et β, quorum tantum ratio spectatur, ac si ambo sint impares, numeri quaesiti per 4 deprimantur:

Numeri quaesiti

I. $\frac{b}{\beta}=\frac{1}{1}$, $p=8$, $q=1$, $r=1$;

II. $\frac{b}{\beta}=\frac{2}{1}$, $p=320$, $q=121$, $r=4$;

III. $\frac{b}{\beta}=\frac{3}{1}$, $p=360$, $q=169$, $r=81$;

IV. $\frac{b}{\beta}=\frac{3}{2}$, $p=7488$, $q=2116$, $r=81$;

V. $\frac{b}{\beta}=\frac{4}{1}$, $p=4352$, $q=2209$, $r=2704$;

VI. $\frac{b}{\beta}=\frac{4}{3}$, $p=57600$, $q=13689$, $r=1936$;

VII. $\frac{b}{\beta}=\frac{5}{1}$, $p=2600$, $q=1369$, $r=12100$.

38. Aliae solutiones reperientur ex his formulis:

$$\frac{aa}{aa+\alpha\alpha}, \quad \frac{(ab-\alpha\beta)^2}{(aa+\alpha\alpha)(bb+\beta\beta)}, \quad \frac{(ab+\alpha\beta)^2}{(aa+\alpha\alpha)(bb+\beta\beta)},$$

quarum summa est

$$\frac{aa}{aa+\alpha\alpha}+1+\frac{aabb+\alpha\alpha\beta\beta-aa\beta\beta-\alpha\alpha bb}{(aa+\alpha\alpha)(bb+\beta\beta)},$$

quae cum unitati aequari debeat, fiet

$$2aabb+\alpha\alpha\beta\beta-\alpha\alpha bb=0, \quad \text{hinc} \quad \frac{aa}{\alpha\alpha}=\frac{bb-\beta\beta}{2bb},$$

seu $$\frac{bb}{\beta\beta}=\frac{\alpha\alpha}{\alpha\alpha-2aa}, \quad \text{unde} \quad b=\alpha \quad \text{et} \quad \beta=\sqrt{(\alpha\alpha-2aa)}.$$

Capiatur ergo:

$$a=2mn, \quad \alpha=mm+2nn, \quad b=mm+2nn, \quad \beta=mm-2nn$$

eruntque tres numeri quaesiti

$$p=8mmnn(m^4+4n^4),$$
$$q=(mm+2mn-2nn)^2(mm+2nn)^2,$$
$$r=(mm-2mn-2nn)^2(mm+2nn)^2,$$

unde sequentes solutiones deducuntur

I. $p=40$, $q=9$, $r=81$;

II. $p=8.9.85$, $q=121.169$, $r=121$;

III. $p=8.4.65$, $q=81.121$, $r=81.9$;

IV. $p=8.36.145$, $q=289.169$, $r=289.121$;

V. $p=8.9.325$, $q=361.529$, $r=361.121$;

VI. $p=8.100.689$, $q=1089.1369$, $r=1089.9$;

VII. $p=8.16.1025$, $q=1089.1521$, $r=1089.529$;

VIII. $p=8.144.1105$, $q=1681.2209$, $r=1681.1$;

IX. $p=8.225.949$, $q=1849.1369$, $r=1849.529$;

39. Neque vero haec solutio generalis est putanda, sed potius innumerabiles aliae locum habent, quae in his geminis formulis non continentur. Pro generali enim solutione hanc aequationem resolvi oporteret:

$$\frac{1}{1+xx}+\frac{1}{1+yy}+\frac{1}{1+zz}=1,$$

unde oritur

$$xxyyzz-xx-yy-zz-2=0$$

hincque $zz=\frac{xx+yy+2}{xxyy-1}$, ita ut haec formula

$$(xxyy-1)(xx+yy+2)$$

in genere ad quadratum reduci debeat, quod quomodo sit efficiendum, non patet.

40. Interim ex solutione jam aliunde cognita, ope hujus formulae infinitae aliae elici possunt. Dividantur enim terni numeri inventi, veluti 40, 9, 81, per eorum summam 130, ut hae fractiones obtineantur:

$$\frac{4}{13},\quad \frac{9}{130},\quad \frac{81}{130},$$

quae cum generalibus comparatae praebent

$$x=\frac{3}{2},\quad y=\frac{11}{3},\quad z=\frac{7}{9},$$

quarum una tantum $x=\frac{3}{2}$ pro cognita sumatur, pro binis reliquis vero haec aequatio resolvatur:

$$\frac{9}{4}yyzz-yy-zz-\frac{17}{4}=0,\quad \text{seu}\quad zz=\frac{4yy+17}{9yy-4},$$

unde fit

$$(9yy-4)z=\sqrt{(9yy-4)(4yy+17)}.$$

Quia autem novimus satisfacere valorem $y=\frac{11}{3}$, statuamus $y=\frac{11+u}{3}$ fitque

$$3(9yy-4)z=\sqrt{(9.13+22u+uu)(49.13+88u+4uu)},$$

ita ut haec formula ad quadratum sit reducenda

$$273^2+22.1105u+3041uu+176u^3+4u^4,$$

cujus radix si statuatur $273+\frac{85.11}{21}u\pm 2uu$, fit

$$\left(\frac{8.13.4489}{21^2}\mp 4.13.21\right)uu+44\left(4\mp\frac{85}{21}\right)u^3=0$$

et $u=-\frac{13(8978\mp 9261)}{11.21(84\mp 85)}$ sicque

$$\text{pro signo superiori}\quad u=\frac{-13.283}{11.21}\quad \text{et}\quad y=\frac{-1138}{693},$$

$$\text{pro signo inferiori}\quad u=\frac{-1403}{231}\quad \text{et}\quad y=+\frac{1138}{693},$$

qui duo valores conveniunt, et ob $y=\frac{1138}{693}$ fit

$$z=\sqrt{\frac{4.1138^2+17.693^2}{9.1138^2-4.693^2}}=\frac{3653}{8.13.30}=\frac{281}{240},$$

unde ternae fractiones prodeunt

$$\frac{4}{13},\quad \frac{480249}{13.136561},\quad \frac{57600}{136561},$$

quae in integris dant hos numeros:

$$p = 4.136561 = 4.17.29.277 = 546244$$
$$q = 480249 = 693^2 = 480249$$
$$r = 13.57600 = 240^2 = 748800$$

hincque

$$p + q + r = 13.17.29.277 = 1775293.$$

Hac ergo methodo solutiones particulares datae ad majorem generalitatem evehuntur.

Casus quatuor numerorum.

41. Statuamus quatuor fractiones:

$$\frac{aa}{aa+\alpha\alpha}, \quad \frac{bb}{bb+\beta\beta}, \quad \frac{(ab-\alpha\beta)^2}{(aa+\alpha\alpha)(bb+\beta\beta)}, \quad \frac{(a\beta-\alpha b)^2}{(aa+\alpha\alpha)(bb+\beta\beta)},$$

quarum summa est

$$\frac{aa}{aa+\alpha\alpha} + \frac{bb}{bb+\beta\beta} + 1 - \frac{4a\alpha b\beta}{(aa+\alpha\alpha)(bb+\beta\beta)}$$

unitati aequanda; unde fit:

$$2aabb + aa\beta\beta + \alpha\alpha bb = 4a\alpha b\beta,$$

ideoque

$$\frac{b}{\beta} = \frac{2a\alpha + \sqrt{(4aa\alpha\alpha - 2a^4 - aa\alpha\alpha)}}{2aa+\alpha\alpha}, \quad \text{seu} \quad \frac{b}{\beta} = \frac{2a\alpha \pm a\sqrt{(3\alpha\alpha - 2aa)}}{2aa+\alpha\alpha}.$$

Quare litteras a et α ita accipi oportet, ut formula $3\alpha\alpha - 2aa$ quadratum evadat.

42. Hunc in finem ponamus:

$$\sqrt{(3\alpha\alpha - 2aa)} = \alpha + \frac{m}{n}(\alpha - a) \quad \text{fietque} \quad 2nn\alpha + 2nna = 2mn\alpha + mm\alpha - mma.$$

Ergo $a = mm + 2mn - 2nn$ et $\alpha = mm + 2nn$, hinc

$$\alpha - a = -2mn + 4nn \quad \text{et} \quad \sqrt{(3\alpha\alpha - 2aa)} = -mm + 4mn + 2nn.$$

Quocirca habebimus

$$\text{vel} \quad \frac{b}{\beta} = \frac{(mm+2mn-2nn)(3mm-4mn+2nn)}{2(mm+2mn-nn)^2+(mm+2nn)^2} = \frac{mm+2mn-2nn}{mm+4mn+6nn},$$

$$\text{vel} \quad \frac{b}{\beta} = \frac{(mm+2mn-2nn)(mm+4mn+6nn)}{2(mm+2mn-2nn)^2+(mm+2nn)^2} = \frac{mm+2mn-2nn}{3mm-4mn+2nn}.$$

Tandem numeri quaesiti habebuntur

$$p = aa(bb+\beta\beta), \quad q = bb(aa+\alpha\alpha), \quad r = (ab-\alpha\beta)^2, \quad s = (a\beta-\alpha b)^2.$$

43. Cum sit $\alpha = mm + 2nn$, loco α alii numeri assumi nequeunt, nisi qui sint vel primi hujus formae $8m+1$, seu $8m+3$, vel ex hujusmodi primis compositi. Simpliciores cum numeris α et $\sqrt{(3\alpha\alpha - 2aa)}$ ipsis respondentibus in sequenti tabella exhibeo:

	$\alpha = 1$	3	9	11	11	17	17	19	19
	$a = 1$	1	11	1	13	11	13	11	23
	$\gamma = 1$	5	1	19	5	25	23	29	5
	$\beta = 3$	11	323	123	459	531	627	603	1419
	$b = 3$	1	187	3	221	99	143	99	759
vel	$b = 1$	11	209	41	351	649	741	737	989
vel	$\beta = 1$	1	19	3	17	9	11	9	33
	$b = 1$	1	11	1	13	11	13	11	23
vel	$\beta = 3$	11	17	41	27	59	57	67	43
	$b = 1$	1	11	1	13	11	13	11	23

44. Cum ergo in genere sit:

$$a = mm + 2mn - 2nn, \quad b = mm + 2mn - 2nn,$$
$$\alpha = mm + 2nn, \quad \beta = mm + 4mn + 6nn,$$
$$\text{vel} \quad \beta = 3mm - 4mn + 2nn,$$

erit

$$ab - \alpha\beta = -8nn(m+n)^2, \quad \text{vel} \quad = -2mm(m-2n)^2,$$
$$\alpha\beta - ab = 4n(m+n)(mm + 2mn - 2nn),$$
$$\text{vel} \quad = 2m(m-2n)(mm + 2mn - 2nn).$$

Item

$$aa + \alpha\alpha = 2mm(m+n)^2 + 2nn(m-2n)^2$$

et

$$bb + \beta\beta = 2(m+n)^2(m+2n)^2 + 2nn(m+4n)^2,$$
$$\text{vel} \quad = 2mm(2m-n)^2 + 2(m-n)^2(m-2n)^2,$$

unde in numeris sequentes nanciscimur solutiones:

I.	$p = 1$,	$q = 1$,	$r = 0$,	$s = 0$,
II.	$p = 5$,	$q = 1$,	$r = 2$,	$s = 2$,
III.	$p = 61$,	$q = 5$,	$r = 512$,	$s = 32$,
IV.	$p = 841$,	$q = 61$,	$r = 225.450$	$s = 450$;
V.	$p = 121.205$,	$q = 121.101$,	$r = 16.32$,	$s = 121.32$;
VI.	$p = 121.289$,	$q = 121.101$,	$r = 25.50$,	$s = 121.50$;
VII.	$p = 121.2305$,	$q = 121.241$,	$r = 576.1152$,	$s = 121.1152$;
VIII.	$p = 169.229$,	$q = 169.145$,	$r = 9.18$,	$s = 169.18$;
IX.	$p = 169.449$,	$q = 169.145$,	$r = 64.128$,	$s = 169.128$.

45. Formulae generales autem ita se habebunt

vel

$$p = (mm(m+n)^2 + nn(m-2n)^2)(mm + 2mn - 3nn)^2,$$
$$q = ((m+n)^2(m+2n)^2 + nn(m+4n)^2)(mm + 2mn - 2nn)^2,$$
$$r = 8nn(m+n)^2(mm + 2mn - 2nn)^2,$$
$$s = 8nn(m+n)^2 \, 4nn(m+n)^2;$$

vel

$$p = (mm(m+n)^2 + nn(m-2n)^2)(mm+2mn-2nn)^2,$$
$$q = (mm(2m-n)^2 + (m-n)^2(m-2n)^2)(mm+2mn-2nn)^2,$$
$$r = 2mm(m-2n)^2(mm+2mn-2nn)^2,$$
$$s = 2mm(m-2n)^2 mm(m-2n)^2.$$

Utroque casu quatuor numeri p, q, r, s ita sunt comparati, ut quilibet in summam trium reliquorum ductus producat numerum quadratum. Quanquam autem hic innumerabiles solutiones derivare licet, haec solutio nonnisi pro maxime particulari est habenda.

46. Solutio autem generaliter instruitur, ponendo in genere pro quaternis fractionibus:

$$\frac{1}{1+zz}, \quad \frac{1}{1+yy}, \quad \frac{1}{1+xx}, \quad \frac{1}{1+vv},$$

quarum summa cum unitati esse debeat aequalis, orietur haec aequatio

$$vvxxyyzz = \begin{cases} vvxx + vvyy + vvzz + 2vv + 2xx + 3 \\ + yyzz + xxzz + xxyy + 2yy + 2zz, \end{cases}$$

cujus autem resolutio maximis difficultatibus est implicata. Verum si ex jam inventis solutionibus, pro binis litteris x et v idonei valores accipiantur, praeter valores reliquarum y et z cognitos innumerabiles alii assignari poterunt.

47. Ut hoc exemplo ostendam, assumam solutionem secundam his fractionibus $\frac{1}{2}$, $\frac{1}{10}$, $\frac{1}{5}$, $\frac{1}{5}$ contentam, indeque statuo $v = 2$ et $x = 3$, reliquas autem, quae hoc exemplo sunt $y = 1$ et $z = 2$ ut incognitas specto. Habebimus ergo hanc aequationem

$$36yyzz = yyzz + 15yy + 15zz + 65,$$

seu

$$7yyzz = 3yy + 3zz + 13,$$

ex qua prodit $zz = \frac{3yy+13}{7yy-3}$, ita ut haec formula $\frac{3yy+13}{7yy-3}$ quadrato aequari debeat, quod duobus casibus $y = 1$ et $y = 2$ evenire novimus. Jam $7yy - 3$ in genere fit quadratum ponendo $y = \frac{mm+3}{mm+4m-3}$, qui in $3yy + 13$ substitutus dat

$$16m^4 + 104m^3 + 148mm - 312m + 144 = \square,$$

cujus radix posita $\quad 4mm + 13m + 12, \quad$ dat $\quad m = -\frac{16}{3}$

at radix posita $\quad 4mm - 13m + 12, \quad$ dat $\quad m = \frac{9}{16}$

utrinque reperitur $\quad y = \frac{283}{37} \quad$ et $\quad z = \frac{254}{273}$.

48. Quanquam autem hoc modo ex inventa quavis solutione continuo alias novas elicere licet, tamen sic mox ad numeros praegrandes pervenitur; quod eo majus est incommodum, cum aliunde solutiones multo simpliciores obtineri queant; id quod quidem nulla certa methodo, sed mero tentamine praestatur: Considerantur scilicet plures fractiones hujus formae $\frac{aa}{aa+uu}$, ex quibus quippe quatuor eligi oportet, quarum summa unitati aequetur: Ita sumtis fractionibus, quarum denominatores in 130 continentur:

$$\frac{1}{2}, \quad \frac{1}{5}, \quad \frac{1}{10}, \quad \frac{4}{13}, \quad \frac{1}{26}, \quad \frac{1}{65}, \quad \frac{16}{65}, \quad \frac{9}{130}, \quad \frac{49}{130},$$
$$\frac{4}{5}, \quad \frac{9}{10}, \quad \frac{9}{13}, \quad \frac{25}{26}, \quad \frac{64}{65}, \quad \frac{49}{65}, \quad \frac{121}{130}, \quad \frac{81}{130},$$

binarum $\frac{9}{130}$ et $\frac{49}{130}$ summa est $\frac{29}{65}$, huic addatur $\frac{16}{65}$, proditque $\frac{45}{65}=\frac{9}{13}$, quae cum $\frac{4}{13}$ producit unitatem. Ita quatuor fractiones

$$\frac{4}{13}, \quad \frac{16}{65}, \quad \frac{9}{130}, \quad \frac{49}{130}$$

praebent hos numeros

$$p=40, \quad q=32, \quad r=9, \quad s=49.$$

Alio modo fit

$$\frac{9}{130}+\frac{1}{5}=\frac{35}{130}=\frac{7}{26}, \quad \text{porro} \quad \frac{7}{26}+\frac{1}{26}=\frac{4}{13},$$

quae cum $\frac{9}{13}$ dat unitatem, unde ex fractionibus

$$\frac{9}{130}, \quad \frac{1}{5}, \quad \frac{1}{26}, \quad \frac{9}{13}$$

nascuntur hi numeri

$$p=9, \quad q=26, \quad r=5, \quad s=90,$$

qui utique multo sunt minores, quam superiores certa ratione inventi, primis quidem ibi exceptis, qui ob aequales numeros excludendi videntur.

49. Simili modo posita summa $p+q+r+s=170$ reperiuntur duae solutiones:

$$\text{I.} \quad p=1, \quad q=10, \quad r=34, \quad s=125;$$
$$\text{II.} \quad p=10, \quad q=17, \quad r=45, \quad s=98;$$

summa numerorum 290 dat

$$p=1, \quad q=40, \quad r=121, \quad s=128.$$

Hinc itaque patet, casu quasi fortuito multo simpliciores numeros problemati satisfacientes reperiri, atque adeo hac ratione non difficulter quinque numeri assignari possunt, ut quilibet per reliquorum summam multiplicatus praebeat numerum quadratum, cujusmodi sunt:

$$2, \quad 40, \quad 45, \quad 58, \quad 145$$
$$\text{et} \quad 32, \quad 61, \quad 98, \quad 169, \quad 250.$$

Hocque modo etiam plures numeros hujus indolis detegere licet, ad quos inveniendos nulla certa methodus adhuc est explorata.

Appendix.

50. Si problemati modo tractato haec conditio adjungatur, ut singuli numeri esse debeant quadrati, quaestionis quasi natura immutatur, quae ita enunciabitur:

Invenire quotcunque numeros quadratos, ut summa omnium quolibet imminuta fiat numerus quadratus.

Sint numeri quadrati quaesiti

$$A^2, \quad B^2, \quad C^2, \quad D^2, \quad \text{etc.},$$

quorum summa ponatur $=S$, fierique debet

$$S - A^2 = P^2, \quad S - B^2 = Q^2, \quad S - C^2 = R^2 \text{ etc.}$$

unde patet, S esse summam ejusmodi binorum quadratorum, quae pluribus modis in bina quadrata se distribui patiatur; seu posito $S = xx + yy$, hanc duorum quadratorum summam indefinite in alia bina quadrata secari oportet, quod in genere ita praestatur:

$$S = \left(\frac{2fx + (ff-1)y}{ff+1}\right)^2 + \left(\frac{(ff-1)x - 2fy}{ff+1}\right)^2 = xx + yy.$$

51. Pro casu ergo trium quadratorum poni debet:

$$A = x, \quad B = \frac{2fx - (ff-1)y}{ff+1} \quad \text{et} \quad C = \frac{2gx - (gg-1)y}{gg+1}$$

et summa quadratorum tum ipsi $xx + yy$ aequari. Quod cum in genere difficulter praestetur, in solutionem particularem inquiramus ponendo $g = \frac{f+1}{f-1}$, unde fit

$$C = \frac{(ff-1)x - 2fy}{ff+1},$$

et haec oritur aequatio:

$$xx + xx + yy - \frac{8f(ff-1)}{(ff+1)^2} xy = xx + yy,$$

ex qua sequitur

$$x = \frac{8f(ff-1)}{(ff+1)^2} y, \quad \text{seu} \quad x = 8f(ff-1) \quad \text{et} \quad y = (ff+1)^2$$

hincque quadratorum quaesitorum radices in integris

$$A = 8f(ff-1)(ff+1),$$
$$B = 2f(3f^4 - 10ff + 3) = 2f(3ff-1)(ff-3),$$
$$C = (ff-1)(f^4 - 14ff + 1) = (ff-1)(ff+4f+1)(ff-4f+1),$$

unde si $f = 2$, sequuntur hi numeri

$$A = 16.3.5, \quad B = 4.11.1, \quad C = 3.13.3,$$
$$\text{seu} \quad A = 240, \quad B = 44, \quad C = 117.$$

52. Ad casum autem quatuor quadratorum progrediamur, quandoquidem tum problema fit difficillimum, ut solutio adeo simplicissima jam ad maximos numeros exsurgat. Faciamus ergo

$$A = x, \quad B = \frac{2fx - (ff-1)y}{1+ff}, \quad C = \frac{(ff-1)x - 2fy}{1+ff}, \quad D = \frac{2px - (pp-1)y}{pp+1},$$

et cum sit

$$BB + CC = xx + yy - \frac{8f(ff-1)xy}{(1+ff)^2},$$

posito brevitatis ergo $\frac{4f(ff-1)}{(ff+1)^2} = g$, prodit haec aequatio:

$$xx + \frac{4ppxx - 4p(pp-1)xy + (pp-1)^2 yy}{(pp+1)^2} - 2gxy = 0,$$

seu $(pp-1)^2 yy = 2g(pp+1)^2 xy - 4ppxx + 4p(pp-1)xy - (pp+1)^2 xx$

hincque

$$\frac{(pp-1)^2 y}{x} = g(pp+1)^2 + 2p(pp-1)$$
$$\pm \sqrt{(gg(pp+1)^4 + 4gp(pp-1)(pp+1)^2 + 4pp(pp-1)^2 - (pp-1)^2(pp+1)^2 - 4pp(pp-1)^2)}$$
$$= g(pp+1)^2 + 2p(pp-1) \pm (pp+1)\sqrt{(gg(pp+1)^2 + 4gp(pp-1) - (pp-1)^2)}.$$

53. Haec formula rationalis reddenda insigni molestia premi videtur, quam autem ponendo $p = \frac{q+1}{q-1}$ tollere licet. Facilior vero redditur solutio, si pro primo numero sumatur $A = y$, unde fit:

$$4ppxx = 2g(pp+1)^2 xy - (pp-1)^2 yy + 4p(pp-1)xy - (pp+1)^2 yy$$

hincque

$$\frac{4ppx}{y} = g(pp+1)^2 + 2p(pp-1) \pm (pp+1)\sqrt{(gg(pp+1)^2 + 4gp(pp-1) - 4pp)},$$

ubi quantitas rationalis reddenda est

$$ggp^4 + 4gp^3 + (2gg-4)pp - 4gp + gg,$$

cujus radix posita $gpp + 2p + g$ dat $p = -g$, ita ut sit

$$\frac{4ggx}{y} = g(gg+1)^2 - 2g(gg-1) \pm (gg+1)(g^3 - g),$$

$$\text{seu} \quad \frac{4gx}{y} = (gg+1)^2 - 2(gg-1) \pm (gg+1)(gg-1).$$

Ergo

$$\text{vel} \quad \frac{4gx}{y} = 2(g^4+1), \quad \text{vel} \quad \frac{4gx}{y} = 4.$$

54. Evolvamus primo posteriorem solutionem utpote simpliciorem, et ob $\frac{y}{x} = \frac{g}{1}$ et $p = -g$ habebitur:

$$A = g, \quad B = \frac{2f - g(ff-1)}{ff+1}, \quad C = \frac{ff - 1 - 2fg}{ff+1}, \quad D = \frac{-2g - g(gg-1)}{gg+1},$$

seu $D = -g$; forent ergo duo quadrata A^2 et D^2 inter se aequalia scilicet

$$A = D = g = \frac{4f(ff-1)}{(ff+1)^2},$$

et pro reliquis

$$B = \frac{2f(f^4 - 6ff + 1)}{(ff+1)^3} \quad \text{et} \quad C = \frac{(ff-1)(f^4 - 6ff + 1)}{(ff+1)^3},$$

quae radices per $(ff+1)^3$ multiplicando ad numeros integros revocatae fient

$$A = D = 4f(ff-1)(ff+1), \quad B = 2f(f^4 - 6ff + 1), \quad C = (ff-1)(f^4 - 6ff + 1),$$

unde sumto $f = 2$ oritur haec solutio:

$$A = 8.3.5, \quad D = 8.3.5, \quad B = 4.7, \quad C = 3.7,$$

$$\text{seu} \quad A = 120, \quad D = 120, \quad B = 28, \quad C = 21.$$

55. Si aequalitas duorum numerorum minus placet, evolvamus alteram solutionem $\frac{x}{y} = \frac{g^4+1}{2g}$, unde fit $x = g^4 + 1$, $y = 2g$, et ob $p = -g$ erit

$$A = 2g,$$

$$B = \frac{2f(g^4+1) - 2g(ff-1)}{ff+1},$$

$$C = \frac{(ff-1)(g^4+1) - 4fg}{ff+1}$$

$$\text{et} \quad D = \frac{-2g(g^4+1) - 2(gg-1)g}{gg+1} = 2g^3,$$

$$\text{seu}\quad A = 2g(ff+1),$$
$$B = 2f(g^4+1) - 2g(ff-1),$$
$$C = (ff-1)(g^4+1) - 4fg,$$
$$D = 2g^3(ff+1),$$

ubi $g = \frac{4f(ff-1)}{(ff+1)^2}$, seu ponatur $g = \frac{m}{n}$ et omnibus ad integros reductis fiet

$$A = 2mn^3(ff+1),$$
$$B = 2f(m^4+n^4) - 2mn^3(ff-1),$$
$$C = (ff-1)(m^4+n^4) - 4fmn^3,$$
$$D = 2m^3n(ff+1).$$

Hinc sumto $f = 2$, ut sit $g = \frac{24}{25} = \frac{m}{n}$, erunt quatuor quadratorum radices:

$$A = 2^4.3.5^7 \quad = 3750000,$$
$$B = 2^3.7.22843 = 639604,$$
$$C = 3^3.7.13219 = 832797,$$
$$D = 2^{10}.3^3.5^3. \quad = 3456000.$$

56. Ob hos numeros tam grandes problema eo magis est attentione dignum, quamobrem operae pretium videtur, adhuc aliam ejus solutionem etsi particularem proponere. Positis igitur quatuor quadratis quaesitis vv, xx, yy, zz, primo has duas tantum conditiones considero:

$$vv + yy + zz = \square \quad \text{et} \quad xx + yy + zz = \square,$$

quibus ut satisfaciam, assumo binos numeros a et α ut sit $aa + \alpha\alpha = AA$, ac statuo

$$vv + yy + zz = \frac{Av + \alpha x}{a}$$
$$xx + yy + zz = \frac{Ax + \alpha v}{a}$$

ut utrinque eadem prodeat aequatio

$$aa(yy+zz) = \alpha\alpha(vv+xx) + 2\alpha Avx;$$

simili modo pro binis reliquis conditionibus pono

$$yy + vv + xx = \frac{Ay - \alpha z}{a}$$
$$zz + vv + xx = \frac{Az - ay}{a}$$

prodibitque hinc

$$\alpha\alpha(vv+xx) = aa(yy+zz) - 2Aayz,$$

quae duae aequationes additae dant

$$\alpha vx = ayz, \quad \text{hincque} \quad z = \frac{\alpha vx}{ay},$$

qui valor in priori substituatur fietque

$$aayy + \frac{\alpha\alpha vvxx}{yy} - \alpha\alpha vv - \alpha\alpha xx - 2\alpha Avx = 0,$$
$$\text{seu}\quad \alpha\alpha xx(vv-yy) = 2\alpha Avxyy + \alpha\alpha vvyy - aay^4$$
$$\text{et}\quad \alpha x = \frac{Avyy \pm y\sqrt{(AAvvyy + aav^4 - aavvyy - aavvy^2 + aay^4)}}{vv-yy},$$

quae ob $AA=\alpha\alpha+aa$ abit in

$$\frac{ax}{y}=\frac{Avy\pm\sqrt{(\alpha\alpha v^4+aay^4)}}{vv-yy}.$$

57. Ponatur $v=y(1+s)$, et cum fiat

$$\sqrt{(\alpha\alpha v^4+aay^4)}=yy\sqrt{(AA+4\alpha\alpha s+6\alpha\alpha ss+4\alpha\alpha s^3+\alpha\alpha s^4)}$$

statuatur haec radix $=A+\frac{2\alpha\alpha}{A}s+\alpha ss$ eritque

$$6\alpha\alpha ss+4\alpha\alpha s^3=\left(\frac{4\alpha^4}{AA}+2\alpha A\right)ss+\frac{4\alpha^3}{A}s^3$$

hincque $$s=\frac{A^3-3\alpha AA+2\alpha^3}{2\alpha A(A-\alpha)}=\frac{AA-2\alpha A-2\alpha\alpha}{2\alpha A}.$$

Quare $\frac{v}{y}=\frac{AA-2\alpha\alpha}{2\alpha A}$ et radix illa

$$=A+\frac{\alpha(AA-2\alpha A-2\alpha\alpha)}{AA}+\frac{(AA-2\alpha A-2\alpha\alpha)^2}{4\alpha AA}$$

$$=A+\frac{(AA-2\alpha A+2\alpha\alpha)(AA-2\alpha A-2\alpha\alpha)}{4\alpha AA}$$

$$=\frac{A^4+4\alpha\alpha AA-4\alpha^4}{4\alpha AA}.$$

Porro est $vv-yy=\frac{(AA+2\alpha A-2\alpha\alpha)(AA-2\alpha A-2\alpha\alpha)}{4\alpha\alpha AA}yy$, hincque

$$\frac{(AA+2\alpha A-2\alpha\alpha)(AA-2\alpha A-2\alpha\alpha)}{4\alpha AA}\cdot\frac{x}{y}=\frac{AA-2\alpha\alpha}{2\alpha}\pm\frac{(A^4+4\alpha\alpha AA-4\alpha^4)}{4\alpha AA}$$

$$=\text{ vel }\frac{A^4-8\alpha\alpha AA+4\alpha^4}{4\alpha AA}=\frac{(AA+2\alpha A-2\alpha\alpha)(AA-2\alpha A-2\alpha\alpha)}{4\alpha AA},\quad\text{vel }\frac{3A^4-4\alpha^4}{4\alpha AA}.$$

Consequenter habebimus

$$\text{vel }\frac{x}{y}=1,\quad\text{vel }\frac{x}{y}=\frac{3A^4-4\alpha^4}{(AA-2\alpha\alpha)^2-4\alpha\alpha AA}$$

denique est $\frac{z}{y}=\frac{AA-2\alpha\alpha}{2aA}\cdot\frac{x}{y}$ ob $\frac{v}{y}=\frac{AA-2\alpha\alpha}{2\alpha A}$.

58. Duas igitur adepti sumus solutiones, quarum prior ita se habet: sumto $y=2\alpha aA$

$$v=a(AA-2\alpha\alpha),$$
$$x=2\alpha aA,$$
$$y=2\alpha aA,$$
$$z=\alpha(AA-2\alpha\alpha),$$

unde sumendo $\alpha=3$, $a=4$ et $A=5$ prodit solutio simplicissima

$$v=28,\quad x=120,\quad y=120,\quad z=21.$$

Altera autem solutio in numeris integris dat

$$v=a(AA-2\alpha\alpha)(AA+2\alpha A-2\alpha\alpha)(AA-2\alpha A-2\alpha\alpha),$$
$$x=2\alpha aA(3A^4-4\alpha^4),$$
$$y=2\alpha aA(AA+2\alpha A-2\alpha\alpha)(AA-2\alpha A-2\alpha\alpha),$$
$$z=\alpha(AA-2\alpha\alpha)(3A^4-4\alpha^4).$$

Unde sumtis $\alpha=3$, $a=4$, $A=5$ solutio simplicissima emergit

$$v = 4 \cdot 7 \cdot 37 \cdot 23 \quad = 23828,$$
$$x = 8 \cdot 3 \cdot 5 \cdot 1551 \quad = 186120,$$
$$y = 8 \cdot 3 \cdot 5 \cdot 37 \cdot 23 = 102120,$$
$$z = 3 \cdot 7 \cdot 1551 \quad = 32571,$$

quorum numerorum quadrata sunt

$$vv = 567773584,$$
$$xx = 34640654400,$$
$$yy = 10428494400,$$
$$zz = 1060870041,$$

reperiturque

$$xx + yy + zz = 214779^2, \quad vv + yy + zz = 109805^2,$$
$$vv + xx + zz = 190445^2, \quad vv + xx + yy = 213628^2,$$
$$\text{et} \quad vv + xx + yy + zz = 25.\ 1201.\ 1555297.$$

59. Quo ratio harum formularum clarius perspiciatur, notari convenit esse:

$$3A^4 - 4a^4 = -(AA + 2aA - 2aa)(AA - 2aA - 2aa)$$

unde erit

$$v = a(AA - 2aa)(AA + 2aA - 2aa)(AA - 2aA - 2aa),$$
$$z = a(AA - 2aa)(AA + 2aA - 2aa)(AA - 2aA - 2aa),$$
$$x = 2aaA(AA + 2aA - 2aa)(AA - 2aA - 2aa),$$
$$y = 2aaA(AA + 2aA - 2aa)(AA - 2aA - 2aa),$$

sicque patet, numeros a et a inter se permutari, ut natura rei postulat. Quod facilius ex his formulis perspicietur:

$$v = a(aa - aa)(3a^4 + 6aaaa - a^4),$$
$$z = a(aa - aa)(3a^4 + 6aaaa - a^4),$$
$$x = 2aaA(3a^4 + 6aaaa - a^4),$$
$$y = 2aaA(3a^4 + 6aaaa - a^4).$$

Hinc est in genere

$$vv + xx + yy = a^2(a^6 + 13a^4aa + 11aaa^4 + 7a^6)^2,$$
$$xx + yy + zz = a^2(a^6 + 13aaa^4 + 11a^4aa + 7a^6)^2,$$
$$vv + yy + zz = A^2(a^6 - a^4aa + 15aaa^4 + a^6)^2,$$
$$vv + xx + zz = A^2(a^6 - aaa^4 + 15a^4aa + a^6)^2,$$

et summa omnium

$$xx + yy + zz + vv = A^2(a^{12} + 34a^{10}a^2 + 175a^8a^4 + 92a^6a^6 + 175a^4a^8 + 34a^2a^{10} + a^{12}),$$

quae in hos factores resolvitur:

$$A^2(a^4 + 6a^2a^2 + a^4)(a^8 + 28a^6a^2 + 6a^4a^4 + 28a^2a^6 + a^8),$$

60. Neque tamen hae formulae minimos numeros suppeditant; sequenti enim modo minores reperiuntur. Ut formula

$$aav^4 + aay^4$$

fiat quadratum, sumtis similibus numeris b et β, ut sit

$$bb + \beta\beta = BB,$$

statuatur

$$\alpha vv = \beta M \quad \text{et} \quad ayy = bM,$$

seu $\frac{vv}{yy} = \frac{a\beta}{\alpha b}$, ut fiat

$$\sqrt{(aav^4 + aay^4)} = BM = \frac{aB}{b} yy,$$

ubi necesse est, ut $\frac{a}{\alpha} \cdot \frac{\beta}{b}$ sit quadratum. Sit ergo

$$\frac{a}{\alpha} \cdot \frac{\beta}{b} = \frac{mm}{nn}, \quad \text{eritque} \quad \frac{v}{y} = \frac{m}{n}$$

tum

$$\frac{x}{y} = \frac{\frac{Am}{n} \pm \frac{aB}{b}}{\alpha\left(\frac{a\beta}{\alpha b} - 1\right)} = \frac{Abm \pm aBn}{a\beta n - \alpha bn} \quad \text{et} \quad \frac{z}{y} = \frac{\alpha m}{an} \cdot \frac{x}{y} = \frac{\beta\,(Abm \pm aBn)}{bm\,(a\beta - \alpha b)}.$$

Jam ponatur

$$a = 21, \quad \alpha = 20, \quad A = 29, \quad b = 35, \quad \beta = 12 \quad \text{et} \quad B = 37,$$

eritque

$$\frac{mm}{nn} = \frac{21}{20} \cdot \frac{12}{35} = \frac{9}{25},$$

ut sit $m = 3$ et $n = 5$, unde colligitur:

$$\frac{v}{y} = \frac{3}{5}, \quad \frac{x}{y} = \frac{29.35.3 \pm 37.21.5}{-5.4.7.16} = \frac{3(-29 \mp 37)}{64} \quad \text{et} \quad \frac{z}{y} = \frac{3(-29 \mp 37)}{16.7}.$$

Pro signo inferiori ergo erit

$$\frac{v}{y} = \frac{3}{5}, \quad \frac{x}{y} = \frac{3}{8} \quad \text{et} \quad \frac{z}{y} = \frac{3}{14},$$

unde in integris

$v = 8.3.7 = 168$	$\sqrt{(xx + yy + zz)} = 305$
$x = 3.5.7 = 105$	$\sqrt{(vv + yy + zz)} = 332$
$y = 8.5.7 = 280$	$\sqrt{(vv + xx + zz)} = 207$
$z = 4.3.5 = 60$	$\sqrt{(vv + xx + yy)} = 343$

$$vv + xx + yy + zz = 121249 = 29.37.113.$$

Hujusmodi autem formulae generales sunt:

$$v = 4fg\,(f + g)\,(3f - g)\,(3ff + gg),$$
$$y = 4fg\,(f - g)\,(3f + g)\,(3ff + gg),$$
$$x = (ff - gg)\,(9ff - gg)\,(3ff + gg),$$
$$z = 2fg\,(ff - gg)\,(9ff - gg).$$

XXXIII.

Observationes circa bina biquadrata, quorum summam in duo alia biquadrata resolvere liceat.

(N. Comment. XVII. 1772. p. 64. Exhib. 1772 Jan. 13.)

1. Quum demonstratum sit, neque summam neque differentiam duorum biquadratorum quadratum esse posse(*), multo minus biquadratum esse poterit; haud minori autem fiducia negari solet, summam trium adeo biquadratorum unquam biquadratum esse posse, etiamsi hoc nusquam demonstratum reperiatur. Utrum autem quatuor biquadrata reperire liceat, quorum summa sit biquadratum, merito dubitamus, quum a nemine adhuc talia biquadrata sint exhibita.

2. Quamvis autem demonstrari posset, non dari terna biquadrata, quorum summa quoque sit biquadratum, id tamen neutiquam ad differentias extendere liceret, neque enim propterea affirmari posset, talem aequationem $A^4 + B^4 - C^4 = D^4$ esse impossibilem; observavi enim hanc aequationem adeo infinitis modis resolvi posse. Neque tamen asseverare ausim, hoc a nemine adhuc esse praestitum, et nunc quidem minime vacat, omnia monumenta in hoc analysis genere evolvere; quicquid autem sit, spero, methodum, qua sum usurus, non omni attentione fore indignam. Manifestum autem est, hanc quaestionem versari circa bina biquadratorum paria, quorum sive summae sive differentiae inter se sint aequales; si enim fuerit $A^4 + B^4 = C^4 + D^4$, utique etiam erit $A^4 - D^4 = C^4 - B^4$; unde hoc problema nobis sit propositum.

3. **Problema.** Invenire bina biquadrata A^4 et B^4, quorum summam in alia duo biquadrata resolvere liceat, it ut habeatur talis aequalitas $A^4 + B^4 = C^4 + D^4$.

Solutio. Quum igitur hinc esse debeat $A^4 - D^4 = C^4 - B^4$, ponamus

$$A = p + q, \quad D = p - q, \quad C = r + s \quad \text{et} \quad B = r - s$$

ut prodeat ista aequatio concinnior

$$pq\,(pp + qq) = rs\,(rr + ss),$$

cui quidem satisfieri liquet, sumendo $r = p$ et $s = q$; verum inde nihil plane lucraremur, quum oriatur casus per se obvius $C = A$ et $B = D$; interim tamen hic ipse casus ad alias solutiones manuducere valet.

4. Jam statuamus:

$$p = ax, \quad q = by, \quad r = kx \quad \text{et} \quad s = y$$

ut obtineatur ista aequatio resolvenda

(*) Vide supra pag. 24 in Commentatione V

$$ab\,(aaxx + bbyy) = k\,(kkxx + yy)$$

unde statim deducimus

$$\frac{yy}{xx} = \frac{k^3 - a^3 b}{ab^3 - k},$$

quam ergo fractionem quadratum reddi oportet. Hic autem statim in oculos incurrit casus, quo hoc usu venit, scilicet sumendo $k = ab$, tum enim fit

$$\frac{yy}{xx} = \frac{a^3 b\,(bb-1)}{ab\,(bb-1)} = aa,$$

unde fieret $y = a$, $x = 1$, hincque $p = a$, $q = ab$, $r = ab$, $s = a$, qui valores producunt ipsum illum casum per se obvium.

5. Hunc igitur casum prosequentes, statuamus $k = ab\,(1 + z)$, et aequatio nostra transfundetur in hanc formam

$$\frac{yy}{xx} = \frac{a^3 b\,((bb-1) + 3bbz + 3bbz^2 + bbz^3)}{ab\,(bb - 1 - z)} = aa\,\frac{(bb - 1 + 3bbz + 3bbz^2 + bbz^3)}{bb - 1 - z}$$

atque ex hac aequatione elicimus

$$\frac{y}{x} = \frac{a\sqrt{((bb-1)^2 + (3bb-1)(bb-1)z + 3bb(bb-2)z^2 + bb(bb-4)z^3 - bbz^4)}}{bb - 1 - z}.$$

Quo igitur formulam:

$$(bb-1)^2 + (bb-1)(3bb-1)\,z + 3bb\,(bb-2)\,zz + bb\,(bb-4)\,z^3 - bbz^4$$

ad quadratum perducamus, statuamus ejus radicem $= bb - 1 + fz + gzz$, et litteras f et g ita assumamus, ut terni termini priores destruantur; quare quum hujus formae quadratum sit:

$$(bb-1)^2 + 2\,(bb-1)\,fz + 2\,(bb-1)\,gzz + ffzz + 2fgz^3 + ggz^4,$$

primi quidem termini se sponte destruunt; ut autem idem in secundis eveniat, sumi debet

$$f = \frac{3bb-1}{2},$$

atque pro tertiis habebimus

$$3bb\,(bb-2) = 2\,(bb-1)\,g + \frac{9b^4 - 6bb + 1}{4},$$

unde colligitur

$$g = \frac{3b^4 - 18bb - 1}{8\,(bb-1)},$$

quibus valoribus definitis, aequatio resolvenda fit

$$(gg + bb)\,z = bb\,(bb-4) - 2fg$$

unde colligimus

$$z = \frac{bb\,(bb-4) - 2fg}{bb + gg}.$$

6. Hinc igitur littera b adhuc arbitrio nostro permittitur; ea igitur pro lubitu assumta, simul atque hinc quantitatem z determinaverimus, statim habebimus

$$x = bb - 1 - z \quad \text{et} \quad y = a\,(bb - 1 + fz + gzz)$$

hincque porro

$$p = a\,(bb - 1 - z), \qquad r = ab\,(1 + z)\,(bb - 1 - z),$$
$$q = ab\,(bb - 1 + fz + gzz), \qquad s = a\,(bb - 1 + fz + gzz),$$

quae formulae quum omnes sint per a divisibiles, eam divisione tollere licebit, ita ut sit

$$p = bb - 1 - z, \qquad r = b(1+z)(bb-1-z),$$
$$q = b(bb - 1 + fz + gzz), \qquad s = bb - 1 + fz + gzz,$$

ubi notandum, si numeri x et y communem habuerint factorem, eum divisione ante tolli posse, quam litterae p, q, r, s inde definiuntur. Operae igitur pretium erit, solutiones quasdam speciales evolvere; at vero statim apparet, sumi non posse $b = 1$, quia fieret $g = \infty$; multo vero minus ponere licet $b = 0$, quia fieret $q = 0$; ex quo casus expediamus duos tantum, primo scilicet $b = 2$, tum vero $b = 3$.

Prima solutio specialis.

7. Sit $b = 2$ ac superiores valores colliguntur, ut sequitur:

$$f = \frac{11}{2}, \quad g = -\frac{25}{24}, \quad z = \frac{6600}{2929},$$

deinde quia littera a plane non in computum ingreditur, ejus loco unitas scribatur, tum vero erit

$$x = 3 - \frac{6600}{2929} = \frac{2187}{2929}, \quad y = 3 + \frac{11}{2}\cdot\frac{6600}{2929} - \frac{25}{24}\cdot\frac{6600^2}{2929^2} = 3 + \frac{55407.1100}{2929^2} = \frac{3.28894941}{2929^2},$$

totum autem negotium redit ad rationem inter x et y, quae quum sit

$$\frac{y}{x} = \frac{3.28894941}{2187.2929} = \frac{28894941}{2929.729} = \frac{3210549}{2929.81} = \frac{1070183}{27.2929},$$

habebimus

$$x = 79083 \quad \text{et} \quad y = 1070183,$$

tum igitur ob

$$k = 2(1+z) = \frac{2.9529}{2929} = \frac{19058}{2929},$$

concludimus fore

$$p = 79083, \qquad r = 27.19058 = 514566,$$
$$q = 2.1070183 = 2140366, \qquad s = 1070.183.$$

Consequenter pro ipsis radicibus biquadratorum nanciscimur

$$A = p + q = 2219449, \qquad C = 1584749,$$
$$B = r - s = -555617, \qquad D = 2061283,$$

eritque propterea $A^4 + B^4 = C^4 + D^4$.

Secunda solutio specialis.

8. Sit $b = 3$ eritque $f = 13$, $g = \frac{5}{4}$ hinc $z = \frac{200}{169}$, ideoque

$$k = \frac{3.369}{169} = \frac{1107}{169} = \frac{9.123}{169} = \frac{27.41}{169}, \quad \text{porro} \quad x = \frac{8.144}{169} = \frac{128.9}{169}$$

$$y = 8 + \frac{200}{169}\left(13 + \frac{5}{4}\cdot\frac{200}{169}\right) = 8 + \frac{200}{169}\cdot\frac{2447}{169} = \frac{8.150911}{169^2}$$

sicque erit

$$x:y = 8 \, . \, 144 \, . \, 169 : 8 \, . \, 150911 = 144 \, . \, 169 : 150911$$

ideoque

$$x = 144 \, . \, 169 = 24336 \quad \text{et} \quad y = 150911,$$

ex quibus valoribus consequimur

$$p = 24335, \quad r = 159408 = 144 \, . \, 1107,$$
$$q = 452733, \quad s = 150911.$$

Atque hinc ipsae litterae A, B, C, D colliguntur

$$A = 477069, \quad C = 310319,$$
$$B = 8497, \quad D = 428397,$$

eritque iterum $A^4 + B^4 = C^4 + D^4$, atque hi numeri videntur minimi quaestioni nostrae satisfacientes.



XXXIV.

Observationes circa divisionem quadratorum per numeros primos.

(Op. anal. I. p. 64. Exhib. 1772?)

§ 1. **Hypothesis.** Si numerorum a, b, c, d, etc. quadrata a^2, b^2, c^2, d^2, etc. per numerum quempiam primum P dividantur, residua in divisione relicta litteris cognominibus graecis α, β, γ, δ, etc. indicemus.

§ 2. **Coroll. 1.** Cum ergo quadratum aa per numerum P divisum relinquat residuum α; posito quoto $= A$, erit $aa = AP + \alpha$, ideoque $aa - \alpha$ divisibile erit per P; similique modo hae expressiones: $bb - \beta$, $cc - \gamma$, $dd - \delta$, etc. divisibiles erunt per eundem divisorem P.

§ 3. **Coroll. 2.** Quadrata $(a + P)^2$, $(a + 2P)^2$, $(a + 3P)^2$, et in genere $(a + nP)^2$ idem residuum α relinquent, si per numerum propositum P dividantur. Unde patet, numerorum, divisore P majorum, quadrata eadem praebere residua, quae ex quadratis numerorum, divisore P minorum, nascuntur.

§ 4. **Coroll. 3.** Cum deinde quadratum $(P - a)^2$ per P divisum idem praebeat residuum, quod quadratum a^2, patet si fuerit $a > \frac{1}{2}P$, fore $P - a < \frac{1}{2}P$. Unde manifestum est, omnia residua diversa ex quadratis numerorum, qui semisse divisoris P sint minores, resultare.

§ 5. **Coroll. 4.** Quare si omnia residua desiderentur, quae ex divisione quadratorum per datum divisorem P proveniunt, sufficiet ea tantum quadrata considerasse, quorum radices semissem ipsius P non superent.

§ 6. **Coroll. 5.** Hinc si divisor sit $P = 2p + 1$, si per eum omnes numeri quadrati 1, 4, 9, 16, 25, etc. dividantur, plura residua diversa inde prodire nequeunt, quam unitates in numero p continentur; eaque resultant ex quadratis numerorum 1, 2, 3, 4, ... p: sequentium enim numerorum $p + 1$, $p + 2$, $p + 3$, etc. quadrata eadem residua ordine retrogrado reproducunt.

§ 7. **Scholion.** Manifestum hoc inde est, quod haec duo quadrata: p^2 et $(p + 1)^2$, per numerum $2p + 1$ divisa, idem praebent residuum; siquidem eorum differentia per $2p + 1$ est divisibilis. Generatim enim, quorumcunque numerorum differentia $M - N$ per $2p + 1$ est divisibilis, necesse est, ut uterque M et N, seorsim divisus, idem residuum relinquat. Hinc etiam cum sit $(p + 2)^2 - (p - 1)^2 = 3(2p + 1)$, utrumque quadratum seorsim, $(p + 2)^2$ et $(p - 1)^2$, idem residuum praebere debet, et in genere quadratum $(p + n + 1)^2$ idem residuum dabit, quod quadratum $(p - n)^2$. Hoc igitur ostenso perspicuum est plura residua resultare non posse, quam in numero p unitates continentur: utrum autem haec residua omnia sint diversa, an quaepiam inter se conveniant? hinc non definitur; atque adeo, si divisores quicunque admittantur, utrumque evenire potest. Sin autem divisor $2p + 1$ fuerit numerus primus, omnia illa residua erunt inter se diversa, quod sequenti modo demonstro.

§ 8. **Theorema I.** Si divisor $P = 2p + 1$ fuerit numerus primus, per eumque omnia quadrata 1, 4, 9, 16, ... usque ad p^2 dividantur, omnia residua hinc resultantia inter se erunt diversa, eorumque adeo multitudo $= p$.

Demonstratio. Sint a et b duo numeri quicunque ipso p minores, vel saltem non majores; ac demonstrandum est, si eorum quadrata a^2 et b^2 per numerum primum $2p + 1$ dividantur, residua certe diversa esse proditura. Si enim idem praebent residuum, eorum differentia $aa - bb$ per $2p + 1$ foret divisibilis, ideoque ob $2p + 1$ numerum primum et $aa - bb = (a + b)(a - b)$, alter horum factorum per $2p + 1$ divisibilis esse deberet. Cum autem sit tam $a < p$ quam $b < p$, saltem non $a > p$, summa $a + b$, multoque magis differentia $a - b$ divisore $2p + 1$ est minor; indeque neutra per $2p + 1$ divisibilis esse potest. Ex quo manifesto sequitur: omnia quadrata, quorum radices non sint ipso p majores, per numerum primum $2p + 1$ divisa, certe diversa residua esse relictura.

§ 9. **Coroll. 1.** Quodsi ergo omnia quadrata 1, 4, 9, 16, etc. per numerum primum $2p + 1$ dividantur, omniaque residua diversa notentur, eorum numerus neque major erit, neque minor quam p, sed huic numero p praecise aequalis.

§ 10. **Coroll. 2.** Omnia vero haec residua diversa numero p, oriuntur ex totidem quadratis in serie naturali primum occurrentibus, scilicet 1, 4, 9, 16, ... pp; neque ex sequentibus majoribus ulla nova residua eliciuntur.

§ 11. **Coroll. 3.** Non omnes ergo numeri ipso divisore $2p + 1$ minores inter residua occurrent, sed tantum tot eorum, quot unitates continentur in divisoris minori semisse p. Quare cum numerorum, divisore $2p + 1$ minorum, multitudo sit $= 2p$, horum alter semissis tantum in ordine residuorum reperietur, alter vero inde penitus excluditur.

§ 12. **Scholion.** Numeros hos divisore primò $2p + 1$ minores, qui ex ordine residuorum excluduntur, nomine *non-residuorum* indicabo, quorum ergo multitudo semper numero residuorum est aequalis. Hoc discrimen inter residua et non-residua probe perpendisse juvabit, quare pro divisoribus aliquot primis minoribus tam residua quam non-residua hic exhibebo.

Divisor 3; $p = 1$		divisor 5; $p = 2$		divisor 7; $p = 3$		divisor 11; $p = 5$	
quadr.	1	quadr.	1, 4	quadr.	1, 4, 9	quadr.	1, 4, 9, 16, 25
resid.	1	resid.	1, 4	resid.	1, 4, 2	resid.	1, 4, 9, 5, 3
non-resid.	2	non-resid.	2, 3	non-resid.	3, 5, 6	non-resid.	2, 6, 7, 8, 10

divisor 13; $p = 6$		divisor 17; $p = 8$	
quadr.	1, 4, 9, 16, 25, 36	quadrata	1, 4, 9, 16, 25, 36, 49, 64
resid.	1, 4, 9, 3, 12, 10	resid.	1, 4, 9, 16, 8, 2, 15, 13
non-resid.	2, 5, 6, 7, 8, 11	non-resid.	3, 5, 6, 7, 10, 11, 12, 14

divisor 19;	$p = 9$
quadrata	1, 4, 9, 16, 25, 36, 49, 64, 81
resid.	1, 4, 9, 16, 6, 17, 11, 7, 5
non-resid.	2, 3, 8, 10, 12, 13, 14, 15, 18

Circa haec residua et non-residua pro quovis divisore primo tam memorabiles proprietates obser-

vantur, quas eo majori studio perpendisse operae est pretium, quod inde non contemnenda incrementa in numerorum theoriam redundare videntur.

§ 13. **Theorema II.** Si in ordine residuorum ex divisore P ortorum occurrant numeri α et β, ibidem quoque occurret eorum productum $\alpha\beta$, siquidem minus fuerit divisore P; sin autem sit majus, ejus loco capi convenit $\alpha\beta - P$, vel $\alpha\beta - 2P$, vel generatim $\alpha\beta - nP$, donec infra P deprimatur.

Demonstratio. Oriantur residua α et β ex divisione quadratorum aa et bb per divisorem P facta, ita ut sit

$$aa = AP + \alpha \quad \text{et} \quad bb = BP + \beta.$$

Hinc erit

$$aabb = ABP^2 + (A\beta + B\alpha) P + \alpha\beta.$$

Quare si quadratum $aabb$ per divisorem P dividatur, residuum relinquetur $\alpha\beta$, vel si $\alpha\beta$ superet divisorem P, ejus loco sumi debet residuum, quod ex divisione ipsius $\alpha\beta$ per P facta relinquetur, quod proinde erit vel $\alpha\beta - P$, vel $\alpha\beta - 2P$, vel $\alpha\beta - 3P$, vel generatim $\alpha\beta - nP$, ita ut sit $\alpha\beta - nP < P$.

§ 14. **Coroll. 1.** Si ergo inter residua occurrat numerus α, ibidem quoque occurret $\alpha\alpha$, item α^3, α^4, etc. omnesque adeo ejus potestates, siquidem a singulis ejusmodi multiplum divisoris P subtrahatur, ut residuum minus fiat divisore P.

§ 15. **Coroll. 2.** Cum igitur existente divisore P numero primo $2p + 1$, residuorum numerus sit $= p$; si unius cujuspiam residui α omnes potestates α^0, α^1, α^2, α^3, α^4, etc. per eundem divisorem P dividantur, inde non plura quam p residua diversa resultare possunt.

§ 16. **Coroll. 3.** Hinc sequitur, potestatem α^p, per $P = 2p + 1$ divisam, idem praebere residuum quod $\alpha^0 = 1$, seu residuum fore unitatem, uti alibi ostendi, siquidem divisor $2p + 1$ fuerit numerus primus.

§ 17. **Scholion.** Eximiis proprietatibus, quae hinc deduci possunt, hic uberius evolvendis non immoror, cum hoc jam olim a me sit factum(*). Ea hic tantum principia breviter repetere constitui, quibus indigeo ad novas quasdam residuorum affectiones explicandas, unde insignes nonnullas numerorum proprietates multo expeditius demonstrare liceat. Hunc in finem animadverto, quod quidem per se est perspicuum, quemadmodum residuo $\alpha\beta$ aequivalent numeri $\alpha\beta - P$, $\alpha\beta - 2P$, et in genere $\alpha\beta - nP$, existente P divisore, ita etiam omnes numeros per P divisos, idem residuum relinquentes, in hoc negotio tanquam hoc ipsum residuum spectari posse. Ita in ordine residuorum, pro quocunque divisore P, omnes plane numeri quadrati ipsi occurrere sunt censendi, cum quilibet aa hujusmodi forma $AP + \alpha$ exhiberi queat, ideoque vero residuo α aequivalere sit existimandus. Hinc etiam inter residua numeri negativi admitti poterunt, cum residuo α aequivaleat $\alpha - P$, hocque pacto omnia residua ad numeros semissi divisoris P minores revocare licebit.

§ 18. **Theorema III.** Si in ordine residuorum, ex divisore P ortorum, occurrant bina residua α et β, in eo quoque occurret residuum $\frac{\alpha + nP}{\beta}$, numero n ita assumto, ut $\frac{\alpha + nP}{\beta}$ fiat numerus integer, id quod semper fieri licet.

(*) Vide supra pag. 215 et seqq in Comment. XV.

Demonstratio. Sint aa et bb ea quadrata, quae per P divisa relinquunt residua α et β, ut sit $aa = AP + \alpha$ et $bb = BP + \beta$. Jam quaeratur c, ut sit $c = \frac{a + mP}{b}$ numerus integer, eritque $cc = \frac{aa + 2amP + mmPP}{bb} = \frac{\alpha + (A + 2am + mmP)P}{\beta + BP} =$ numero integro. Cum nunc numerator tanquam ipsum residuum α, denominator vero tanquam residuum β spectari possit, patet, si cc per P dividatur, residuum ad formam propositam reductum iri. Posito enim brevitatis gratia $A + 2am + mmP = D$, ut sit $cc = \frac{\alpha + DP}{\beta + BP}$, tum vero $\frac{\alpha + nP}{\beta} = \gamma$, ostendi oportet, fore $cc = CP + \gamma$, ut residuum ex divisione quadrati cc per numerum P natum prodeat $= \gamma$. Cum autem sit $\alpha = \beta\gamma - nP$, utique fieri poterit:

$$cc = \frac{\beta\gamma + (D - n)P}{\beta + BP} = CP + \gamma,$$

quoniam inde sequitur:

$$(D - n)P = (\beta C + \gamma B + BCP)P,$$

seu $$D - n = \beta C + \gamma B + BCP,$$

cujusmodi relatio inter coefficientes ipsius P omnino necessaria est, ut numeri integri prodeant.

Aliter. Loco residui α aliud aequivalens accipiatur $\alpha + nP$, ut sit $\alpha + nP = \beta\gamma$; et cum omnia quadrata hujus formae $(a + mP)^2$ idem praebeant residuum α, quod ex quadrato aa nasci assumitur, sumatur m ita, ut fiat $a + mP = bc$, et quia quadratum $bbcc$ per P divisum relinquit residuum α, vel $\beta\gamma$, quadratum vero bb residuum β: necesse est ut quadratum cc relinquat residuum $\gamma = \frac{\alpha + nP}{\beta}$. Sit enim $bbcc = EP + \beta\gamma$ et $bb = BP + \beta$; tum vero si neges quadratum cc praebiturum esse residuum γ, praebeat diversum x, ut sit $cc = CP + x$; erit ergo

$$bbcc = EP + \beta\gamma = (BP + \beta)(CP + x) = \beta x + (\beta C + Bx + BCP)P.$$

Jam multiplis divisoris P utrinque omissis, quemadmodum in aestimatione residuorum fieri solet, siquidem in minima forma desiderentur, habebitur $\beta x = \beta\gamma$, ideoque $x = \gamma$.

§ 19. **Coroll. 1.** Cum igitur unitas semper sit residuum, si pro divisore P fuerit aliquod residuum α, tum etiam $\frac{1 + nP}{\alpha}$ inter residua occurret, quod si vocetur β, erit $\alpha\beta = 1 + nP$, seu inter residua productum $\alpha\beta$ unitati aequivalebit.

§ 20. **Coroll. 2.** Pro quolibet ergo residuo α aliud quasi ejus reciprocum β assignari potest, ut $\alpha\beta$ unitati aequivaleat, sumendo scilicet $\beta = \frac{1 + nP}{\alpha}$, atque haec duo residua reciproca α et β inter se erunt diversa, nisi ambo fuerint vel $+ 1$, vel $- 1$. Si enim sit $\beta = \alpha$ et

$$\alpha\alpha = 1 + nP = 1 + 2mP + mmPP,$$

erit $\alpha = \pm (1 + mP)$ et multiplum divisoris mP omittendo, $\alpha = \pm 1$.

§ 21. **Coroll. 3.** Dum igitur in ordine residuorum cuilibet residuo suum reciprocum adjungitur, hoc modo bina copulabuntur; semper autem unitas solitaria relinquetur, tum vero etiam residuum $- 1$, seu $P - 1$, quoties quidem inter residua occurrit.

§ 22. **Scholion.** Idea haec binorum residuorum reciprocorum maximi est momenti, et ad demonstrationem facilem theorematis pulcherrimi nos manuducet, quod alias per satis multas am-

bages demonstraveram(*): scilicet quod numerus primus formae $4q+1$ semper sit summa duorum quadratorum. Ceterum hic meminisse juvabit, si pro quopiam divisore P residua sint α, β, γ, δ, etc. non-residua vero $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc., tum residuorum omnia producta mutua $\alpha\beta$, $\alpha\gamma$, etc. etiam inter residua reperiri, eorum autem producta per quodpiam non-residuum, veluti $\alpha\mathfrak{A}$, inter non-residua esse referenda. At producta ex binis non-residuis, uti $\mathfrak{A}\mathfrak{B}$, in ordinem residuorum transeunt.

§ 23. **Theorema IV.** Si divisor P fuerit numerus primus formae $4q+3$, tum -1, seu $P-1$ certe in ordine non-residuorum reperitur.

Demonstratio. Cum posito divisore $P=2p+1$, hic sit $p=2q+1$, ideoque numerus impar, numerus omnium residuorum erit impar. At si -1 in ordine residuorum occurreret, cuilibet residuo α responderet aliud residuum $-\alpha$, unde ordo residuorum ita se esset habiturus:

$$+1,\quad +\alpha,\quad +\beta,\quad +\gamma,\quad +\delta \quad \text{etc.}$$
$$-1,\quad -\alpha,\quad -\beta,\quad -\gamma,\quad -\delta \quad \text{etc.}$$

foretque ergo numerus residuorum par. Cum igitur numerus residuorum certo sit impar, fieri nequit, ut in ordine residuorum occurrat -1, seu $P-1$, consequenter in ordine non-residuorum necessario reperiri debet.

§ 24. **Coroll. 1.** Quodsi ergo pro divisore primo $P=4q+3$ inter residua occurrat numerus α, tum numerus $-\alpha$, seu $P-\alpha$ certe inter non-residua reperietur; similique modo, si $-\beta$ fuerit residuum, tum $+\beta$ erit non-residuum.

§ 25. **Coroll. 2.** Si quadratum aa per divisorem $P=4q+3$ divisum relinquat residuum α, quia nullum datur quadratum xx, quod praebeat residuum $-\alpha$, fieri omnino nequit, ut ulla summa duorum quadratorum $aa+xx$, per numerum illum $4q+3$ divisibilis, existat.

§ 26. **Coroll. 3.** Oriatur praeterea residuum β ex quadrato bb, et quia forma βaa residuum dat $\alpha\beta$, forma vero αbb residuum $\alpha\beta$, haec forma $\beta aa-\alpha bb$ per divisorem $P=4q+3$ erit divisibilis.

§ 27. **Coroll. 4.** Cum autem nullum detur quadratum xx, quod residuum praebeat $-\beta$, nulla datur forma αxx residuum praebens $-\alpha\beta$, nulla hujusmodi forma $\beta aa+\alpha xx$ per numerum $P=4q+3$ erit divisibilis, siquidem α et β sint residua, et α residuum quadrato aa respondens.

§ 28. **Coroll. 5.** Cum autem neque haec forma $\beta aacc+\alpha ccxx$ per divisorem $P=4q+3$ sit divisibilis, nisi quadratum cc divisionem admittat, qui casus sponte excluditur, quadrato $aacc$ quodcunque aliud residuum praeter α respondere potest; unde, loco $aacc$ et $ccxx$ scribendo dd et yy, nulla hujusmodi forma $\beta dd+\alpha yy$ exhiberi potest per numerum $P=4q+3$ divisibilis, dum α et β sint residua.

§ 29. **Scholion.** Quo haec clarius perspiciantur, percurramus quosdam numeros primos formae $4q+3$, ac residua ejus semisse majora, subtrahendo inde $4q+3$, negative repraesentemus, ut infra semissem revocentur, indeque pateat, nullius residui α negativum $-\alpha$ simul in ordine residuorum occurrere:

(*) Vide supra pag. 163 in Comment. XII.

Divisor	residua
3	1
7	1, −3, +2
11	1, +4, −2, +5, +3
19	1, +4, +9, −3, +6, −2, −8, +7, +5
23	1, +4, +9, −7, +2, −10, +3, −5, −11, +8, +6
31	1, +4, +9, −15, −6, +5, −13, +2, −12, +7, −3, −11, +14, +10, +8.

Hic evidens est, inter residua omnes numeros semisse divisoris non majores occurrere vel signo $+$, vel $-$ affectos, nullum autem bis utroque signo affectum occurrere. Hinc si singulorum horum residuorum signa mutentur, ordo non-residuorum complebitur. Hinc pro divisore 31 sequentes formae exhiberi possunt nunquam per 31 divisibiles: $aa+bb$, $aa-15bb$, $aa-6bb$, $aa+5bb$, $aa-13bb$, $aa+2bb$, $aa+7bb$, $aa-3bb$, $aa-11bb$, $aa+14bb$, $aa+10bb$. Atque in genere, si α et β sint duo quaecunque residua, nulla hujusmodi forma: $\alpha aa+\beta bb$, per numerum 31 divisionem admittet.

§ 30. **Theorema V.** Si divisor P fuerit numerus primus formae $4q+1$, tum numerus -1, seu $P-1$ certe in ordine residuorum reperitur.

Demonstratio. Sit α residuum quodcunque, eritque etiam ejus reciprocum $\frac{1}{\alpha}$, seu $\frac{1+nP}{\alpha}$ residuum (19), quod, nisi sit vel $\alpha=+1$, vel $\alpha=-1$, ab α erit diversum, ita ut exceptis his duobus casibus cuilibet residuo α respondeat suum reciprocum, quod sit α', ab α diversum; ubi notetur ipsius α' reciprocum vicissim esse α. Quare si -1 inter residua non reperiretur, omnia residua ita repraesentari possent, binis reciprocis conjungendis:

$$\begin{array}{cccccc} 1, & \alpha, & \beta, & \gamma, & \delta, & \text{etc.} \\ & \alpha', & \beta', & \gamma', & \delta', & \text{etc.} \end{array}$$

sicque cum omnia sint diversa, numerus omnium residuorum foret impar. Cum autem divisor sit numerus primus formae $4q+1$, numerus omnium residuorum est $2q$, ideoque par; unde necessario sequitur, inter residua quoque numerum -1, seu $P-1$ occurrere, quia alioquin numerus residuorum foret impar.

§ 31. **Coroll. 1.** Cum ergo pro divisore primo $P=4q+1$ numerus -1 certe inter residua reperiatur, si aliud residuum quodcunque fuerit α, inter residua etiam occurret $-\alpha$.

§ 32. **Coroll. 2.** Si igitur quadratum aa per divisorem primum $4q+1$ divisum relinquat residuum α, aliud dabitur quadratum bb, quod residuum praebebit $-\alpha$, unde horum quadratorum summa $aa+bb$ certe erit per numerum primum $4q+1$ divisibilis.

§ 33. **Coroll. 3.** Quoniam omnia residua ex quadratis, quorum radices semissem divisoris non superant, nascuntur, quadrato quocunque proposito aa, aliud semper bb non majus quam $4qq$ exhiberi potest, ut summa $aa+bb$ prodeat divisibilis per $4q+1$.

§ 34. **Coroll. 4.** Si $1 + aa$ divisionem per $4q + 1$ admittat, tum etiam $bb + aabb$, ac proinde quoque $bb + (ab - (4q + 1)n)^2$ divisionem admittet, sicque altero quadrato bb pro lubitu assumto alterum $(ab - (4q + 1)n)^2$ facile reperitur.

§ 35. **Coroll. 5.** Si haec duorum quadratorum summa $aa + bb$ per divisorem $4q + 1$ fuerit divisibilis, tum etiam $aaxx + bbxx$, ac proinde quoque haec forma:

$$(ax - (4q + 1)m)^2 + (bx - (4q + 1)n)^2$$

divisionem admittet. Semper autem x ita assumere licet, ut alterius radix $ax - (4q + 1)m$ dato numero c aequetur, sumendo $x = \frac{c + (4q + 1)m}{a}$, quod semper in integris fieri potest.

§ 36. **Schollon I.** Pro quovis divisore primo, sive sit formae $4q + 1$, sive $4q + 3$, numerorum reciprocorum consideratio omnem attentionem meretur, cum inde tam facile hanc insignem veritatem elicuerimus, quod, proposito numero primo quocunque formae $4q + 1$, semper summae binorum quadratorum exhiberi queant per illum divisibiles. Cum igitur demonstrari praeterea possit, summam duorum quadratorum alios non admittere divisores, nisi qui ipsi sint summae duorum quadratorum, hoc modo theorematis Fermatiani, quod omnes numeri primi formae $4q + 1$ sint duorum quadratorum aggregata, demonstratio multo expeditius absolvitur, quam quidem olim a me est factum. Quemadmodum autem numeri reciproci pro quovis divisore P se habeant, dum cujusvis numeri α reciprocus est $\frac{1 + nP}{\alpha}$, ex subjunctis exemplis clarius intelligetur:

Divisor	Reciprocorum paria
3	. . .
5	2
	3
7	2, 3
	4, 5
11	2, 3, 5, 7
	6, 4, 9, 8
13	2, 3, 4, 5, 6
	7, 9, 10, 8, 11
17	2, 3, 4, 5, 8, 10, 11
	9, 6, 13, 7, 15, 12, 14
19	2, 3, 4, 6, 7, 8, 9, 14
	10, 13, 5, 16, 11, 12, 17, 15
23	2, 3, 4, 5, 7, 9, 11, 13, 15, 17
	12, 8, 6, 14, 10, 18, 21, 16, 20, 19
29	2, 3, 4, 5, 7, 8, 9, 12, 14, 16, 18, 19, 23
	15, 10, 22, 6, 25, 11, 13, 17, 27, 20, 21, 26, 24.

Singula haec paria reciproca ita inter se sunt connexa, ut quilibet numerus unicum tantum recipiat reciprocum, divisore scilicet minorem, prorsus uti in theoremate assumsimus.

§ 37. **Scholion 2.** Quodsi ergo divisor primus fuerit formae $4q+1$, videamus quomodo residua secundum hanc legem reciprocorum disposita se sint habitura:

Divisor	Residua
5	1, 4
	1, (— 1)
13	1, 4, 9, 3, 12, 10
	1, 4, 9, 12
	10, 3, (— 1)
17	1, 4, 9, 16, 8, 2, 15, 13
	1, 4, 9, 8, 16
	13, 2, 15, (— 1)
29	1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22
	1, 4, 9, 16, 25, 6, 23, 28
	22, 13, 20, 7, 5, 24, (— 1)
37	1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28
	1, 4, 9, 16, 25, 12, 27, 26, 21, 36
	28, 33, 7, 3, 34, 11, 10, 30, (— 1)

Ex his exemplis perspicuum est, cum unitas sit solitaria, et reliquorum residuorum quodque suum reciprocum habeat adjunctum, numerum residuorum futurum esse imparem, nisi praeter unitatem aliud residuum solitarium accederet, quod sibi ipsi esset reciprocum. Quoniam igitur his casibus, quibus divisor est numerus primus formae $4q+1$, numerus residuorum certo est par $=2q$, necesse est ut praeter unitatem, residuum $4q$, vel -1 occurrat, cujus quippe reciprocum ipsi est aequale. Unde veritas insignis istius theorematis, cujus demonstratio alioquin maxime erat difficilis, admodum fit perspicua: quod scilicet, quoties divisor sit numerus primus formae $4q+1$, inter residua semper occurrat numerus $4q$, vel -1.

§ 38. **Scholion 3.** Quemadmodum hinc patet numerum -1 inter residua reperiri, quoties divisor fuerit numerus primus formae $4q+1$, ita pro quovis alio numero primo s, divisorum primorum forma assignari, at nondum demonstrari potest, ut iste numerus s in residuis reperiatur. Cujusmodi est hoc theorema:

Si divisor primus fuerit formae $4ns+(2x+1)^2$, *existente* s *numero primo, tum in residuis occurrent numeri* $+s$ *et* $-s$.

alterumque huic simile:

Si divisor primus fuerit formae $4ns-(2x+1)^2$ *existente* s *numero primo, tum in residuis occurret numerus* $+s$; *at* $-s$ *erit in non-residuis.*

Quando autem vicissim $-s$ occurrat in residuis, at $+s$ in non-residuis, ita in genere definiri nequit. Pro casibus autem particularibus res ita se habere deprehenditur:

ut sit	divisor primus debet esse
-2 residuum $+2$ non-residuum	$P = 8n + 3$
-3 residuum $+3$ non-residuum	$P = 12n + 7$
-5 residuum $+5$ non-residuum	$P = 20n + 3,\ 7$
-7 residuum $+7$ non-residuum	$P = 28n + 11,\ 15,\ 23$
-11 residuum $+11$ non-residuum	$P = 44n + 3,\ 15,\ 23,\ 27,\ 31$
-13 residuum $+13$ non-residuum	$P = 52n + 7,\ 11,\ 19,\ 15,\ 31,\ 47$
-17 residuum $+17$ non-residuum	$P = 68n + 3,\ 7,\ 11,\ 23,\ 27,\ 31,\ 39,\ 63$
-19 residuum $+19$ non-residuum	$P = 76n + 7,\ 11,\ 19,\ 23,\ 35,\ 39,\ 43,\ 47,\ 55,\ 63$
-23 residuum $+23$ non-residuum	$P = 92n + 3,\ 23,\ 27,\ 31,\ 35,\ 39,\ 47,\ 55,\ 59,\ 71,\ 75,\ 87.$

Quorum casuum contemplatio hoc suppeditat theorema:

Si divisor primus fuerit formae $4ns - 4z - 1$, *excludendo omnes valores in forma*

$$4ns - (2x + 1)^2$$

contentos, existente s *numero primo, tum in residuis occurret* $-s$, *at* $+s$ *erit non-residuum.*

Quibus theorematibus insuper hoc adjungi potest:

Si divisor primus fuerit formae $4ns + 4z + 1$, *excludendo omnes valores in forma*

$$4ns + (2x + 1)^2$$

contentos, existente s *numero primo, tum tam* $+s$ *quam* $-s$ *in non-residuis occurret.*

Theoremata haec ideo subjungo, ut qui hujusmodi speculationibus delectantur, in eorum demonstrationem inquirant, cum nullum sit dubium, quin inde theoria numerorum insignia incrementa sit adeptura.

§ 39. **Conclusio.** Quatuor haec theoremata postrema, quorum demonstratio adhuc desideratur, sequenti modo concinnius exhiberi possunt:

Existente s *numero quocunque primo, dividantur tantum quadrata imparia* 1, 9, 25, 49, *etc. per divisorem* 4s, *notenturque residua, quae omnia erunt formae* $4q + 1$, *quorum quodvis littera* α *indicetur, reliquorum autem numerorum, formae* $4q + 1$, *qui inter residua non occurrunt, quilibet littera* $\mathfrak{A}$ *indicetur, quo facto si fuerit*

divisor numerus primus formae	*tum est*
$4ns + \alpha$	$+s$ *residuum et* $-s$ *residuum*
$4ns - \alpha$	$+s$ *residuum et* $-s$ *non-residuum*
$4ns + \mathfrak{A}$	$+s$ *non-residuum et* $-s$ *non-residuum*
$4ns - \mathfrak{A}$	$+s$ *non-residuum et* $-s$ *residuum.*

XXXV.

Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta.

(Op. anal. I. 121. Exhib. 1772. Maji 18.)

§ 1. Si numerus quadratus aa per numerum primum p dividatur, residuum relictum littera α indicetur; similique modo litterae β, γ, δ, etc. mihi denotabunt residua in divisione quadratorum bb, cc, dd, etc. relicta.

§ 2. Erit ergo $\alpha = aa - np$, quia residuum α prodit, si a quadrato aa multiplum numeri p auferatur, idque maximum, ut residuum α ipso divisore p minus reddatur. Nihil autem impedit, quominus multiplum np majus accipiatur quadrato aa, unde residuum α prodit negativum, sicque ejus valor infra $\frac{1}{2}p$ deprimi potest.

§ 3. Idem igitur residuum α multis modis exhiberi potest, quoniam cunctae hae formae $\alpha \pm mp$ eandem naturam continent. Perinde scilicet est, sive residuum ex divisione quadrati aa per numerum p ortum dicatur esse α, sive $\alpha \pm p$, sive $\alpha \pm mp$, denotante littera m numerum integrum quemcunque.

§ 4. Innumera autem quadrata aa, per numerum p divisa, idem relinquunt residuum α, quae omnia ex cognito uno aa facile inveniuntur. Cuncta haec quadrata ista forma $(a \pm mp)^2$, vel $(mp \pm a)^2$ contineri evidens est; sicque sufficit residuum ex harum forma minima, cujus radix non excedet $\frac{1}{2}p$, notasse: omnia scilicet hae quadrata $(mp \pm a)^2$ respectu numeri p ejusdem indolis sunt censenda.

§ 5. Quadratis secundum ordinem naturalem dispositis, residua per divisorem p orta ita se habebunt:

Quadrata:	1,	2^2,	3^2,	$4^2, \ldots$	$(p-4)^2$,	$(p-3)^2$,	$(p-2)^2$,	$(p-1)^2$
Residua:	1,	4,	9,	$16, \ldots$	16,	9,	4,	1.

Quadratis ergo ad $(p-1)^2$ continuatis, singula residua bis occurrunt; et quia p est numerus primus, eorum numerus est par, et bina quadrata media $\left(\frac{p-1}{2}\right)^2$ et $\left(\frac{p+1}{2}\right)^2$, idem dabunt residuum $\frac{pp-2p+1}{4}$.

§ 6. Omnia ergo residua, quae quidem ex divisione numerorum quadratorum per numerum primum p resultare possunt, nascuntur ex his quadratis:

$$\text{Quadrata:}\quad 1,\ 2^2,\ 3^2,\ 4^2, \ldots \left(\frac{p-1}{2}\right)^2$$

$$\text{Residua:}\quad 1,\ 4,\ 9,\ 16, \ldots \frac{pp-2p+1}{4},$$

quorum numerus est $=\frac{p-1}{2}$. Neque ergo omnes numeri divisore p minores, quorum multitudo est $p-1$, inter residua occurrunt, sed eorum semissis inde certe excluditur.

§ 7. Continuatis autem quadratis ad $\left(\frac{p-1}{2}\right)^2$, residua inde orta omnia sunt diversa: neque enim ullum usque ad hunc terminum bis occurrere potest, siquidem divisor p sit numerus primus. Namque si bina quadrata aa et bb, neutro quadratum $\left(\frac{p-1}{2}\right)^2$ excedente, idem darent residuum r, differentia eorum $aa-bb$, ideoque vel $a-b$, vel $a+b$, per p dividi posset. Cum autem neque a neque b superet $\frac{p-1}{2}$, etiam summa $a+b$ minor erit quam p, ideoque fieri omnino nequit, ut ea summa, ac multo minus differentia $a-b$, divisionem per numerum p admittat.

§ 8. Proposito ergo numero primo p omnia residua ex his quadratis

$$1,\ 2^2,\ 3^2,\ 4^2 \ldots\ldots \left(\frac{p-1}{2}\right)^2$$

obtinentur, quorum numerus cum sit $=\frac{p-1}{2}$, et residua omnia inter se differant, numerorum ipso p minorum, quorum multitudo est $p-1$, semissis certe inter residua occurrit; semissis vero inde excluditur, et classem non residuorum constituit. Pro quolibet ergo numero primo p residua a non-residuis probe sunt discernenda.

§ 9. Si enim α inter residua occurrat, pronunciare possumus, innumerabilia quadrata dari, quae in hac forma $np+\alpha$ contineantur, ac minimi eorum radicem non excedere numerum $\frac{p-1}{2}$. Sin autem numerus $\mathfrak{A}$ inter residua non reperiatur, pronunciabimus nullum numerum quadratum in forma $np+\mathfrak{A}$ contineri. Quovis autem casu tam residuorum α quam non-residuorum $\mathfrak{A}$ multitudo est $=\frac{p-1}{2}$.

§ 10. Quodsi residua, ex divisione quadratorum per numerum primum p oriunda, secundum hunc ordinem naturalem disponantur, primo occurrent numeri quadrati 1, 4, 9, 16, etc. donec divisione per numerum p ad minores numeros redigi possunt: postremum vero eorum erit $\frac{pp-2p+1}{4}$, unde numerum p, quoties fieri potest, aufferri oportet.

§ 11. Ad hoc postremum residuum agnoscendum duos casus contemplari convenit, prout numerus primus p fuerit formae vel $4q+1$, vel $4q+3$. Sit primo $p=4q+1$, ideoque $\frac{p-1}{2}=2q$, et ultimum residuum $4qq$, quod subtractione multipli $qp=4qq+q$ reducitur ad $-q$, seu ad $3q+1$. Altero vero casu $p=4q+3$, seu $\frac{p-1}{2}=2q+1$, ultimum residuum $4qq+4q+1$ ablatione multipli $qp=4qq+3q$ reducitur ad $q+1$.

§ 12. Simili modo penultimum residuum, ex quadrato $\left(\frac{p-3}{2}\right)^2$ ortum, reperitur:

pro casu $p=4q+1$, $4qq-4q+1$, seu $-5q+1$, seu $-q+2$;
pro casu $p=4q+3$, $4qq+11$, seu $-3q$, seu $q+3$.

At antepenultimum, ex $\left(\frac{p-5}{2}\right)^2$ ortum, ita prodit:

pro casu $p=4q+1$, $4qq-8q+4$, seu $-9q+4$, seu $-q+6$;
pro casu $p=4q+3$, $4qq-4q+1$, seu $-7q+1$, seu $q+7$.

Quod vero antepenultimum praecedit, hoc modo:

$$\text{pro casu} \quad p = 4q + 1, \quad 4qq - 12q + 9, \quad \text{seu} \; -13q + 9, \quad \text{seu} \; -q + 12;$$
$$\text{pro casu} \quad p = 4q + 3, \quad 4qq - 8q + 4, \quad \text{seu} \; -11q - 4, \quad \text{seu} \; q + 13.$$

§ 13. Hos igitur binos casus distinguendo, residua sequenti modo se habebunt:

Casu $p = 4q + 1$.

$$\begin{array}{ll} \text{Quadrata:} & 1,\ 2^2,\ 3^2,\ 4^2 \ldots (2q-3)^2,\ (2q-2)^2,\ (2q-1)^2,\ (2q)^2; \\ \text{Residua:} & 1,\ 4,\ 9,\ 16 \ldots -q+12,\ -q+6,\ -q+2,\ -q, \\ & \text{seu}\ 3q+13,\ 3q+7,\ 3q+3,\ 3q+1. \end{array}$$

Casu $p = 4q + 3$.

$$\begin{array}{ll} \text{Quadrata:} & 1,\ 2^2,\ 3^2,\ 4^2 \ldots (2q-2)^2,\ (2q-1)^2,\ (2q)^2,\ (2q+1)^2; \\ \text{Residua:} & 1,\ 4,\ 9,\ 16 \ldots q+13,\ q+7,\ q+3,\ q+1. \end{array}$$

Priori scilicet casu in genere occurrit residuum $-q + nn + n$, seu $3q + nn + 1$, posteriori vero $q + nn + n + 1$.

§ 14. Quo hic residuorum ordo clarius perspiciatur, exempla spectanda proponam, et primo quidem pro numeris primis formae $p = 4q + 1$.

$p = 5$	1,	2^2
$q = 1$	1,	4
seu	1,	-1

$p = 13$	1,	2^2,	3^2,	4^2,	5^2,	6^2
$q = 3$	1,	4,	9,	3,	12,	10
seu	1,	4,	-4,	3,	-1,	-3

$p = 17$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2
$q = 4$	1,	4,	9,	16,	8,	2,	15,	13
seu	1,	4,	-8,	-1,	8,	2,	-2,	-4

$p = 29$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2,	9^2,	10^2,	11^2,	12^2,	13^2,	14^2
$q = 7$	1,	4,	9,	16,	25,	7,	20,	6,	23,	13,	5,	28,	24,	22
seu	1,	4,	9,	-13,	-4,	7,	-9,	6,	-6,	13,	5,	-1,	-5,	-7

$p = 37$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2,	9^2,	10^2,	11^2,	12^2,	13^2,	14^2,	15^2,	16^2,	17^2,	18^2
$q = 9$	1,	4,	9,	16,	25,	36,	12,	27,	7,	26,	10,	33,	21,	11,	3,	34,	30,	28
seu	1,	4,	9,	16,	-12,	-1,	12,	-10,	7,	-11,	10,	-4,	-16,	11,	3,	-3,	-7,	-9

$p = 41$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2,	9^2,	10^2,	11^2,	12^2,	13^2,	14^2,	15^2,	16^2,	17^2,	18^2,	19^2,	20^2
$q = 10$	1,	4,	9,	16,	25,	36,	8,	23,	40,	18,	39,	21,	5,	32,	20.	10,	2,	37,	33,	31
seu	1,	4,	9,	16,	-16,	-5,	8,	-18,	-1,	18,	-2,	-20,	5,	-9,	20,	10,	2,	-4,	-8,	-10

ubi observare licet, in residuis per negativa ad minimam formam reductis, singulos numeros bis, positive scilicet et negative occurrere.

§ 15. Sequentia exempla pertinent ad numeros primos formae $p = 4q + 3$.

$p = 3$	1
$q = 0$	1

$p = 7$	1,	2^2,	3^2
$q = 1$	1,	4,	2
seu	1,	-3,	2

$p = 11$	1,	2^2,	3^2,	4^2,	5^2
$q = 2$	1,	4,	9,	5,	3
seu	1,	4,	-2,	5,	3

$p = 19$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2,	9^2
$q = 4$	1,	4,	9,	16,	6,	17,	11,	7,	5
seu	1,	4,	9,	-3,	6,	-2,	-8,	7,	5

$p = 23$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2,	9^2,	10^2,	11^2
$q = 5$	1,	4,	9,	16,	2,	13,	3,	18,	12,	8,	6
seu	1,	4,	9,	-7,	2,	-10,	3,	-5,	-11,	8,	6

$p = 31$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2,	9^2,	10^2,	11^2,	12^2,	13^2,	14^2,	15^2
$q = 7$	1,	4,	9,	16,	25,	5,	18,	2,	19,	7,	28,	20,	14,	10,	8
seu	1,	4,	9,	-15,	-6,	5,	-13,	2,	-12,	7,	-3,	-11,	14,	10,	8

$p = 43$	1,	2^2,	3^2,	4^2,	5^2,	6^2,	7^2,	8^2,	9^2,	10^2,	11^2,	12^2,	13^2,	14^2,	15^2,	16^2,	17^2,	18^2,	19^2,	20^2,	21^2
$q = 10$	1,	4,	9,	16,	25,	36,	6,	21,	38,	14,	35,	15,	40,	24,	10,	41,	31,	23,	17,	13,	11
seu	1,	4,	9,	16,	-18,	-7,	6,	21,	-5,	14,	-8,	15,	-3,	-19,	10,	-2,	-12,	-20,	17,	13,	11

In istis residuis ad minimam formam reductis omnes plane numeri ab unitate usque ad $2q + 1$ occurrunt, alii signo positionis, alii negationis affecti. Verum has proprietates observatas demonstrari oportet.

§ 16. Jam supra, p. 479 demonstravi, si inter residua, ex divisione quadratorum per numerum p orta, occurrant numeri α et β, ibidem quoque reperiri productum $\alpha\beta$, ac proinde quoque hanc formam latius patentem $\alpha^m \beta^n$. Oriantur enim haec residua ex quadratis aa et bb, ita ut sit $aa = mp + \alpha$ et $bb = np + \beta$, atque manifestum est ex horum quadratorum producto

$$aabb = mnpp + (m\beta + n\alpha)\,p + \alpha\beta,$$

cujus forma est $Mp + \alpha\beta$, nasci residuum $\alpha\beta$; similique modo ex quadrato $a^{2m} b^{2n}$ provenire residuum $\alpha^m \beta^n$, seu $\alpha^m \beta^n - Mp$, ut ad minimam formam reducatur. Quin etiam notari convenit, hoc ipsum residuum $\alpha^m \beta^n$ nasci ex omnibus his quadratis: $(a^m b^n \pm Np)^2$, seu $(Np \pm a^m b^n)^2$, ideoque ex quadrato, cujus latus $a^m b^n - Np$, seu $Np - a^m b^n$ minus erit quam $\frac{1}{2}p$.

§ 17. Denotent litterae $a, b, c, d, \ldots. l$ omnes numeros divisoris p semisse $\frac{1}{2}p$ minores, quorum ergo multitudo est $= \frac{p-1}{2}$, sintque $\alpha, \beta, \gamma, \delta, \ldots. \lambda$ residua ex eorum quadratorum $a^2, b^2, c^2, d^2, \ldots. l^2$ per numerum p divisione relicta, quorum multitudo itidem est $= \frac{p-1}{2}$, ita

ut ex omnibus numeris divisore p minoribus, quorum multitudo est $p-1$, totidem ex residuorum ordine excludantur, quos nomine non-residuorum complexos litteris $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, ... $\mathfrak{L}$ indicabo. Notatu ergo maxime dignum est, in ordine residuorum α, β, γ, δ, ... λ, etiamsi eorum multitudo tantum est $=\frac{p-1}{2}$, tamen omnia eorumdem producta ex binis pluribusque, atque etiam singulorum potestates omnes occurrere; siquidem auferendo inde, quoties fieri potest, divisorem p, ad minimam formam revocentur.

§ 18. Quo magis haec illustrentur, animadverti oportet, ratione cujusque divisoris p omnes numeros in totidem species distribui; scilicet ratione divisoris 2 duae habentur species numerorum parium et imparium formulis $2x$ et $2x+1$ contentorum. Divisor autem 3 tres praebet numerorum species $3x$, $3x+1$ et $3x+2$, et divisor 4 has quatuor $4x$, $4x+1$, $4x+2$ et $4x+3$, quae diversae species in numerorum doctrina sollicite distingui solent. Simili ergo modo ratione divisoris cujusque p, hae diversae numerorum species constituuntur:

$$px,\quad px+1,\quad px+2,\quad px+3, \ldots. px+p-1,$$

quarum multitudo est p. Omissa ergo prima specie px multipla divisoris p continente, reliquarum multitudo est $p-1$; ac si p fuerit numerus primus, has species in duas classes dividi convenit, utraque $\frac{p-1}{2}$ species complectente:

$$px+\alpha,\quad px+\beta,\quad px+\gamma,\quad px+\delta, \ldots. px+\lambda,$$
$$px+\mathfrak{A},\quad px+\mathfrak{B},\quad px+\mathfrak{C},\quad px+\mathfrak{D}, \ldots px+\mathfrak{L},$$

ita ut omnes numeri quadrati in priori classe contineantur, posterior vero classis naturae quadratorum prorsus adversetur.

§ 19. Pro quolibet ergo divisore primo p his duabus classibus constitutis, quarum utraque $\frac{p-1}{2}$ species continet, et quae ambae conjunctim omnes plane numeros continent, exceptis multiplis ipsius p, quippe quorum judicium est in promtu, omnes numeri in priori classe contenti hac gaudent proprietate, ut producta ex binis in eadem classe contineantur, in qua ergo simul non solum potestates singulorum quaecunque, sed etiam producta ex binis pluribusque harum potestatum occurrunt. Prior igitur classis, quam voco residuorum, numeris α, β, γ, δ, ... λ determinatur, dum altera classis non-residuorum numeris $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, ... $\mathfrak{L}$ definitur.

§ 20. Demonstravi deinde etiam, si in classe residuorum occurrant duo numeri r et rs, quorum ille r hujus rs sit factor, tum etiam hujus alterum factorem in eadem classe reperiri. Cum enim dentur duo quadrata aa et bb, ut formae $aa-r$ et $bb-rs$ sint per numerum primum p divisibiles, existentibus numeris a et b ipso p minoribus, etiam forma $aas-rs$ per p est divisibilis, hincque etiam differentia $bb-aas$, et $(b+np)^2-aas$. Cum autem a et b sint ipso p minores, semper n ita assumere licet, ut fiat $b+np=ma$. Ex quo talis forma $mmaa-aas$ dabitur per p divisibilis, adeoque et haec $mm-s$, ita ut sit $s=mm-np$, ac propterea numerus s inter residua reperiatur. Hinc sequitur, si r fuerit residuum, at s non-residuum, tum productum rs certe fore non-residuum; seu producta ex quovis residuo per non-residuum facta, veluti $\alpha\mathfrak{A}$, $\alpha\mathfrak{B}$, $\beta\mathfrak{A}$ inter non-residua reperiuntur.

§ 21. Si igitur $\mathfrak{A}$ fuerit non-residuum, omnia haec producta: $\alpha\mathfrak{A}$, $\beta\mathfrak{A}$, $\gamma\mathfrak{A}$, ... $\lambda\mathfrak{A}$, erunt non-residua, quae cum sint diversa inter se, etiam reductione ad minimam formam facta, eorumque numerus $=\frac{p-1}{2}$, in iis adeo omnia non-residua continentur. Ex quo jam perspicuum est producta ex binis non-residuis, veluti $\alpha\beta\mathfrak{A}\mathfrak{A}$, ad classem residuorum esse referenda, quoniam $\alpha\beta$ est residuum, et $\mathfrak{A}\mathfrak{A}$, utpote numerus quadratus, per se inter residua occurrit. Simul vero patet producta ex ternis non-residuis, uti $\mathfrak{A}\mathfrak{B}\mathfrak{C}$, iterum in classem non-residuorum cadere, producta vero ex quaternis inter ipsa residua reperiri, et ita porro.

§ 22. Praeterea vero etiam observo ex datis binis residuis α et β per divisionem novum residuum oriri, et fractionem $\frac{\alpha}{\beta}$ inter residua esse referendam. Etsi enim fractiones ex hac ratione prorsus excluduntur, tamen, quia numerus α aequivalens censetur huic formae generali $\alpha+np$, universam speciem continente, numerum n utique ita accipere licet, ut $\frac{\alpha+np}{\beta}$ fiat numerus integer, de quo effatum est intelligendum, quod scilicet inter residua reperiatur. Hinc ergo omnes termini hujus progressionis geometricae:

$$\alpha,\ \beta,\ \frac{\beta^2}{\alpha},\ \frac{\beta^3}{\alpha^2},\ \frac{\beta^4}{\alpha^3},\ \text{etc.}$$

ex binis residuis α et β continuatae, in classe residuorum continentur, si scilicet singuli ad formas integras revocentur. Quodsi enim fractio $\frac{\beta}{\alpha}$ aequivaleat numero integro r, statim sequentes numeri integri obtinentur: α, β, βr, βr^2, βr^3, βr^4, etc. qui ad minimam formam reducti non plures quam $\frac{p-1}{2}$ numeros diversos praebere possunt.

§ 23. Consideremus ergo hanc progressionem geometricam α, β, βr, βr^2, βr^3, βr^4, etc. et cum omnes termini diversi esse nequeant, praebeant hi termini βr^m et βr^{m+n} per p divisi idem residuum, ita ut differentia $\beta r^{m+n}-\beta r^m$, ac propterea r^n-1 per p fiat divisibilis. Tum ergo etiam termini β et βr^n, atque etiam α et βr^{n-1} ratione residui convenient; ex quo patet, plura residua diversa prodire non posse, quam quae oriuntur ex his terminis initialibus:

$$\alpha,\ \beta,\ \beta r,\ \beta r^2,\ \ldots\ \beta r^{n-2},$$

quoniam ex sequentibus βr^{n-1}, βr^n, βr^{n+1}, etc. eadem residua eodem ordine recurrunt; quorum ergo residuorum, siquidem fuerint diversa, multitudo major esse nequit quam $\frac{p-1}{2}$: quod evenit si r^n sit minima potestas ipsius r, quae unitate minuta per p divisionem admittat. Hinc patet numerum n certe non superare $\frac{p-1}{2}$; ac si fuerit $n=\frac{p-1}{2}$, omnia plane residua obtinentur.

§ 24. Sin autem ex terminis α, β, βr, βr^2, ... βr^{n-2}, non omnia residua prodeant, sed quaedam omittantur, facile ostenditur, ad minimum totidem omitti, quot adsunt. Si enim residuum γ inter ea non occurrat, quod etiam per $\alpha\delta$ repraesentare licet, quoniam $\gamma+mp$ semper ad formam $\alpha\delta$ revocari potest, tum etiam neque $\beta\delta$, neque $\beta\delta r$, neque $\beta\delta r^2$, etc. inter ea residua reperietur, quae cum sint diversa, excluso uno simul n excluduntur, unde $2n$ numerum omnium $\frac{p-1}{2}$ superare nequit. Erit ergo vel $2n=\frac{p-1}{2}$, vel $2n<\frac{p-1}{2}$, et posteriori casu adhuc de novo ad minimum n residua excluduntur. Quare cum termini progressionis geometricae

$$\alpha, \beta, \beta r, \beta r^2, \ldots\ldots \beta r^{n-2},$$

quorum numerus est n, vel omnia residua contineant ex quadratis orta, quorum multitudo est $=\frac{p-1}{2}$, vel inde exclusorum numerus sit $=n$, vel $=2n$, vel $=3n$, etc. evidens est numerum n necessario partem aliquotam ipsius $\frac{p-1}{2}$ esse debere, ideoque minimum exponentem n, quo potestas r^n unitate minuta per p divisibilis reddatur, vel ipsi numero $\frac{p-1}{2}$, vel ejusdem parti cuipiam aliquotae esse aequalem.

§ 25. Sive autem sit $n=\frac{p-1}{2}$, sive ejus parti cuidam aliquotae aequetur, semper forma $r^{\frac{1}{2}(p-1)}-1$ divisionem admittet per numerum primum p. Ponamus $p=2q+1$, ut sit $\frac{p-1}{2}=q$; ac si ex binis quadratorum residuis quibuscunque α et β, sumendo $r=\frac{\beta+np}{\alpha}$, formetur haec progressio geometrica:

$$\alpha, \beta, \beta r, \beta r^2, \beta r^3, \ldots\ldots \beta r^{q-2},$$

terminorum numero existente $=q$, tum hinc vel omnia residua quadratorum,

$$\alpha, \beta, \gamma, \delta, \varepsilon, \ldots\ldots \lambda,$$

resultabunt, vel eorum tantum semissis, vel pars tertia, vel pars quarta aliave aliquota: simulque perspicitur, quot ab initio diversa prodierint, eadem deinceps eodem ordine continuo repetitum iri. Semper autem termini sequentes βr^{q-1}, βr^q, βr^{q+1}, etc. eadem residua reproducent α, β, βr, quae initio habentur.

§ 26. Quoties ergo q est numerus primus, existente $p=2q+1$, tum progressio geometrica ex binis quadratorum residuis quibusque α et β formata et ad q terminos continuata:

$$\alpha, \beta, \beta r, \beta r^2, \beta r^3, \ldots\ldots \beta r^{q-2},$$

omnia plane quadratorum residua exhibebit, nullo neque excluso neque repetito. Omnia ergo reliqua residua γ, δ, $\varepsilon, \ldots\ldots \lambda$, cum tali quopiam termino βr^n, ut sit $n<q-1$, convenient. Sin autem numerus q fuerit compositus, puta $q=mn$ et $p=2mn+1$, tum evenire potest, ut non omnia residua quadratorum sic prodeant, sed tantum ejusmodi pars aliquota ipsius q, qualem ejus indoles admittit. Quod si usu venit, tota progressio geometrica, q terminis constans, quasi sponte in duo plurave membra distinguitur, in quibus eadem residua recurrunt.

§ 27. Cum sit $\frac{\beta}{\alpha}=r$, ideoque $\beta=\alpha r$, nostra progressio geometrica hoc modo expressa magis fit perspicua:

$$\alpha, \alpha r, \alpha r^2, \alpha r^3, \ldots\ldots \alpha r^{q-1},$$

cujus omnes termini quia sunt per α multiplicati, hoc factore communi praetermisso, progressio simplicius ita exhiberi potest: $1, r, r^2, r^3, \ldots r^{q-1}$. Proposito scilicet divisore primo $p=2q+1$, si residuum quodcunque fuerit α, singuli termini hujus progressionis geometricae:

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4, \ldots\ldots \alpha^{q-1}$$

quorum numerus est $=q$, inter residua quadratorum reperiuntur; ac si omnes ad diversas species pertineant, etiam universam residuorum classem implent. Fieri autem potest, uti vidimus, ut non omnia residua hoc modo prodeant, sed totius classis tantum pars aliquota, dum eadem post certam periodum iterum repetuntur, reliqua vero hinc prorsus excluduntur.

§ 28. Sive autem omnia quadratorum residua ex hac progressione geometrica nascantur, sive quaedam tantum pars aliquota, ea, quae terminis istius progressionis continentur, tam insignibus proprietatibus sunt praedita, ut operae omnino pretium sit eas accuratius evolvere. Primum igitur observo, si haec progressio geometrica ulterius continuetur, terminos sequentes a^q, a^{q+1}, a^{q+2}, etc. aequivalere primis 1, a, a^2, etc. propterea quod $a^q - 1$ dividi certe potest per divisorem primum $p = 2q + 1$. Adjecto ergo termino sequente a^q unitati aequivalente, ita ut habeamus

$$1,\ a,\ a^2,\ a^3, \ldots\ldots a^{q-3},\ a^{q-2},\ a^{q-1},\ 1$$

quia productum ex primo termino in ultimum est $= 1$, ex natura progressionis geometricae sequitur, etiam producta ex secundo a in penultimum a^{q-1}, item ex tertio a^2 in antepenultimum a^{q-2}, et in genere ex binis ab extremis aequidistantibus a^m et a^{q-m} ad unitatem reduci.

§ 29. Dato ergo quocunque residuo α inter reliqua unum reperietur β, ita ut productum $\alpha\beta$ unitati aequivaleat, seu sit $\beta = \frac{1+np}{\alpha}$, unde id facile invenitur. Quia igitur haec duo residua α et β tali vinculo inter se colligantur, ea *sociata* nominabo; ex quo superioris progressionis geometricae bini termini ab extremis aequidistantes hujusmodi bina residua *sociata* suppeditant. Terminus scilicet penultimus a^{q-1} aequivalet ipsi β, antepenultimus a^{q-2} ipsi β^2 et ita porro, unde si sociata subscribantur hoc modo:

$$1,\ a,\ a^2,\ a^3, \ldots\ldots a^{q-3},\ a^{q-2},\ a^{q-1},\ 1$$
$$1,\ \beta,\ \beta^2,\ \beta^3, \ldots\ldots \beta^{q-3},\ \beta^{q-2},\ \beta^{q-1},\ 1$$

inferior series congruit cum superiori retro scripta. Semper autem residuum unitati associatum quoque est unitas.

§ 30. Consideratio horum residuorum sociatorum aperit nobis viam ad insignes proprietates detegendas. Cum enim, posito divisore primo $p = 2q + 1$, sit numerus omnium residuorum $= q$, quorum cuilibet, praeter unitatem, convenit suum sociatum, unitate exclusa reliqua, quorum numerus est $= q - 1$, secundum hanc sociationem in paria distribui possunt, binis sociatis invicem jungendis. Hinc si $q - 1$ fuerit numerus impar, ac propterea q par, necesse est, ut in hac distributione idem residuum, puta δ, bis occurrat. Verum idem residuum δ duobus diversis residuis associari nequit: si enim esset $\alpha\delta = 1$ et $\beta\delta = 1$, residua α et β non discreparent. Quare nihil aliud relinquitur, nisi ut idem residuum δ secum ipsum associetur, sitque idcirco $\delta\delta = 1$, unde fit vel $\delta = 1$, vel $\delta = -1$; sed quia unitas jam est seposita, necesse est hoc casu, quo q est numerus par, inter residua reperiri -1, vel $p - 1$.

§ 31. En ergo egregiam demonstrationem veritatis supra jam observatae, quod si divisor primus sit $p = 4m + 1$, ideoque $q = 2m$, inter residua necessario occurrat -1, seu semper exhiberi queat quadratum aa, ut $aa + 1$ per illum numerum primum $p = 4m + 1$ dividi possit. Hinc simul patet, si inter residua sit numerus α, ibidem quoque productum $-1.\alpha$, nempe $-\alpha$ occurrere, hincque omnia residua ad minimam formam reducta tam positive quam negative adesse, omnino uti in exemplis § 14 allatis perspicitur. Simul vero etiam patet, si fuerit $p = 4m + 3$, ideoque residuorum multitudo impar, ibi -1 locum habere non posse, quia tum singula residua utroque signo $+$ et $-$ occurrerent, ideoque eorum numerus impar esse non posset. Ex quo sequitur, per hujusmodi numerum primum $p = 4m + 3$ nullam binorum quadratorum summam dividi posse.

§ 32. Pro divisoribus autem primis formae $p = 4m + 1$, si quadratum aa det residuum α, aliud semper dabitur quadratum bb, praebens residuum $-\alpha$; sicque horum quadratorum summa $aa + bb$ per illum numerum primum erit divisibilis, ita ut nec a nec b superet $2m$. Operae pretium ergo erit his casibus bina residua signo discrepantia junctim exhibere, simulque quadrata, unde nascuntur, adscribere.

$p = 5$	
	1^2
+	$+1$
−	-1
	2^2

$p = 13$			
	1^2	2^2	4^2
+	$+1$	$+4$	$+3$
−	-1	-4	-3
	5^2	3^2	6^2

$p = 17$				
	1^2	6^2	2^2	5^2
+	$+1$	$+2$	$+4$	$+8$
−	-1	-2	-4	-8
	4^2	7^2	8^2	3^2

$p = 29$							
	1^2	2^2	11^2	8^2	6^2	3^2	10^2
+	$+1$	$+4$	$+5$	$+6$	$+7$	$+9$	$+13$
−	-1	-4	-5	-6	-7	-9	-13
	12^2	5^2	13^2	9^2	14^2	7^2	4^2.

$p = 37$									
	1^2	15^2	2^2	9^2	3^2	11^2	14^2	7^2	4^2
+	$+1$	$+3$	$+4$	$+7$	$+9$	$+10$	$+11$	$+12$	$+16$
−	-1	-3	-4	-7	-9	-10	-11	-12	-16
	6^2	16^2	12^2	17^2	18^2	8^2	10^2	5^2	13^2

$p = 41$										
	1^2	17^2	2^2	13^2	7^2	3^2	16^2	4^2	10^2	15^2
+	$+1$	$+2$	$+4$	$+5$	$+8$	$+9$	$+10$	$+16$	$+18$	$+20$
−	-1	-2	-4	-5	-8	-9	-10	-16	-18	-20
	9^2	11^2	18^2	6^2	19^2	14^2	20^2	5^2	8^2	12^2

§ 33. Hinc evidens est, pro divisore primo $p = 4m + 1$ tot modis, quot m continet unitates, bina quadrata, radices limitem $2m$ non superantes habentia, assignari posse, quorum summa sit divisibilis per numerum p. In his autem binis quadratis nulla lex, qua inter se cohaereant, perspicitur, aliorumque summa modo major reperitur modo minor, ac minima quidem ubique ipsi numero p est aequalis. Num autem semper talis binorum quadratorum summa divisori p aequalis detur, hinc non facile demonstrari posse videtur. Cum autem ex alio fonte demonstraverim, binorum quadratorum summam alios non admittere divisores, nisi qui ipsi sint binorum quadratorum summae (*), quoniam hic evictum est semper dari binorum quadratorum summas, quae sint per numerum primum $p = 4m + 1$ divisibiles, jam certo constat omnes numeros primos formae $4m + 1$ esse summam duorum quadratorum. Praesens autem supplementum demonstrationem hujus propositionis mirifice contrahit. Olim enim nonnisi per multas ambages ostendi, dari semper ejusmodi binorum quadratorum summas, quae sint per quemlibet numerum primum formae $4m + 1$ divisibiles, id quod hic in aprico est positum.

§ 34. Data autem duorum quadratorum summa $aa + bb$ per numerum primum p divisibili, alias inde binorum quadratorum summas idem praestantes facile reperire licet.

(*) Comment. XII pag. 161.

1. Si numeri a et b communem habeant divisorem, ut sit $a = nc$ et $b = nd$, etiam summa quadratorum $cc + dd$ per p erit divisibilis.

2. Si numeri a et b ambo sint impares, ideoque $\frac{a+b}{2}$ et $\frac{a-b}{2}$ numeri integri, etiam horum quadratorum summa per p divisionem admittet: semissis autem ea est praecedentis.

3. Tum vero etiam hae quadratorum summae: $(p-a)^2 + (p-b)^2$, vel $a^2 + (p-b)^2$ per p erunt divisibiles; unde si radices communem sortiantur divisorem, eo ad formam minorem redigi possunt.

4. Si ergo sint ambo impares $a = 2c + 1$ et $b = 2d + 1$, ob $p = 4m + 1$, horum quadratorum summa $(2m - c)^2 + (2m - d)^2$ erit per p divisibilis; et si alter par $a = 2c$, alter impar $b = 2d + 1$, haec summa $cc + (2m - d)^2$ erit per p divisibilis; hocque modo continuo plures hujusmodi binorum quadratorum summas invenire licet.

§ 35. Exemplo haec fient clariora. Sumto igitur divisore $p = 41$, inventa sit summa duorum quadratorum $17^2 + 11^2$ per eum divisibilis, ut sit $a = 17$ et $b = 11$; atque per has regulas sequentes valores alii pro a et b reperientur:

$p = 41$, $a = 17 \ldots\ldots 24$	$4 \ldots 4$	$1 \ldots 40$	5
$b = 11 \ldots\ldots 30$	$5 \ldots 36$	$9 \ldots 32$	4

Tum vero porro ex casu, quo alteruter numerorum est $= 1$, alteri valor quicunque tribui, alterque ita definiri potest, ut infra $\frac{1}{2}p$ subsistat. Scilicet invento casu $a = 1$ et $b = 9$, satisfacit quoque $a = m$ et $b = 9m$, ubi loco b sumi potest $9m - np$, seu $np - 9m$, ita ut b infra $\frac{1}{2}p$ deprimatur; sicque pro a omnes numeros accipere licebit.

$a = 1$,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16,	etc.
$b = 9$,	18,	14,	5,	4,	13,	19,	10,	1,	8,	17,	15,	6,	3,	12,	20,	etc.

Desideratur ergo methodus, inter omnes hos binos valores litterarum a et b eos inveniendi, quorum quadratorum summa sit minima, ut deinceps demonstretur, hanc summam ipsi divisori 41 certe fore aequalem: quod quidem praesenti casu evenit, si litterarum a et b valores sint 4 et 5.

§ 36. Revertor autem ad eam residuorum ex quadratis oriundorum dispositionem, qua ea secundum progressionem geometricam disponi posse observavi. Sit igitur divisor primus $p = 2q + 1$, et residua inde ex quadratis orta ordine quocunque scripta $1, \alpha, \beta, \gamma, \delta \ldots \lambda$, quorum multitudo est $= q$, atque sequentes progressiones geometricae omnes in his residuis continebuntur:

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4, \ldots\ldots \alpha^{q-1},$$
$$1,\ \beta,\ \beta^2,\ \beta^3,\ \beta^4, \ldots\ldots \beta^{q-1},$$
$$1,\ \gamma,\ \gamma^2,\ \gamma^3,\ \gamma^4, \ldots\ldots \gamma^{q-1},$$
$$1,\ \delta,\ \delta^2,\ \delta^3,\ \delta^4, \ldots\ldots \delta^{q-1},$$

etc.

in quibus omnibus termini sequentes $\alpha^q, \beta^q, \gamma^q, \delta^q \ldots \lambda^q$ unitati aequivalebunt, quippe qui omnes unitate minuti per divisorem p erunt divisibiles. Hujusmodi ergo progressiones geometricas tot

exhibere licet, quot unitates in q continentur; in iisque omnibus nullus terminus occurret, qui non inter residua $1, \alpha, \beta, \gamma \ldots . \lambda$ reperiatur.

§ 37. Evenire autem potest, ut supra est ostensum, ut non omnes istae progressiones geometricae, etiamsi cujusque terminorum numerus sit $= q$, omnia residua praebeant, sed tantum eorum vel semissem, vel trientem, vel etiam quampiam partem aliquotam; quod quibus casibus contingat, accuratius est perpendendum. Primum igitur observo, si q fuerit numerus primus, hoc nullo modo usu venire posse; si enim in hujusmodi progressione geometrica q terminorum non omnia residua occurrant, eorum quae occurrunt singula vel bis, vel ter, vel aliquoties occurrant necesse est. Unde si q est numerus primus, quaelibet progressio geometrica omnia residua diversa numero q complectitur. Ita si $p = 11$ et $q = 5$, ex quinque residuis $1, 4, -2, 5, 3$, ab unitate incipiendo hae quatuor progressiones geometricae formantur:

	$1,$	$4,$	$4^2,$	$4^3,$	4^4		$1,$	$-2,$	$2^2,$	$-2^3,$	2^4
seu	$1,$	$4,$	$5,$	$-2,$	3	seu	$1,$	$-2,$	$4,$	$3,$	5
	$1,$	$5,$	$5^2,$	$5^3,$	5^4		$1,$	$3,$	$3^2,$	$3^3,$	3^4
seu	$1,$	$5,$	$3,$	$4,$	-2	seu	$1,$	$3,$	$-2,$	$5,$	4

ubi singula residua per omnia loca variantur praeter primum.

§ 38. Hinc evidens est, ex qualibet harum progressionum geometricarum reliquas facile formari posse, dum ex illa, per saltum transiliendo vel unum, vel duos, vel plures terminos, termini excerpuntur, hac numeratione, cum ad finem fuerit perventum, iterum ab initio instituta. Ita si casum sumamus, quo $p = 23$ et $q = 11$, ac residua $1, 4, 9, -7, 2, -10, 3, -5, -11, 8, 6$, una progressione geometrica formata, cujus terminis indices inscribo, quo deinceps reliquae, terminis per saltum excerpendis, facilius exhiberi queant, decem progressiones geometricae ita se habebunt:

													Seq.
1.	Indices	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10;	0
	progr.	1,	4,	$-7,$	$-5,$	3,	$-11,$	2,	8,	9,	$-10,$	6;	1
2.	indices	0,	2,	4,	6,	8,	10,	1,	3,	5,	7,	9;	0
	progr.	1,	$-7,$	3,	2,	9,	6,	4,	$-5,$	$-11,$	8,	$-10;$	1
3.	indices	0,	3,	6,	9,	1,	4,	7,	10,	2,	5,	8;	0
	progr.	1,	$-5,$	2,	$-10,$	4,	3,	8,	6,	$-7,$	$-11,$	9;	1
4.	indices	0,	4,	8,	1,	5,	9,	2,	6,	10,	3,	7;	0
	progr.	1,	3,	9,	4,	$-11,$	$-10,$	$-7,$	2,	6,	$-5,$	8;	1
5.	indices	0,	5,	10,	4,	9,	3,	8,	2,	7,	1,	6;	0
	progr.	1,	$-11,$	6,	3,	$-10,$	$-5,$	9	$-7,$	8,	4,	2;	1
6.	indices	0,	6,	1,	7,	2,	8,	3,	9,	4,	10,	5;	0
	progr.	1,	2,	4,	8,	$-7,$	9,	$-5,$	$-10,$	3,	6,	$-11;$	1

													Seq.
7.	indices	0,	7,	3,	10,	6,	2,	9,	5,	1,	8,	4;	0
	progr.	1,	8,	−5,	6,	2,	−7,	−10,	−11,	4,	9,	3;	1
8.	indices	0,	8,	5,	2,	10,	7,	4,	1,	9,	6,	3;	0
	progr.	1,	9,	−11,	−7,	6,	8,	3,	4,	−10,	2,	−5;	1
9.	indices	0,	9,	7,	5,	3,	1,	10,	8,	6,	4,	2;	0
	progr.	1,	−10,	8,	−11,	−5,	4,	6,	9,	2,	3,	−7;	1
10.	indices	0,	10,	9,	8,	7,	6,	5,	4,	3,	2,	1;	0
	progr.	1,	6,	−10,	9,	8,	2,	−11,	3,	−5,	−7,	4;	1.

Indices scilicet hic ultra 11 ascensuri subtrahendo 11 sunt depressi. Hic porro observari convenit bina residua, quorum indices juncti faciunt 11, seu in genere q, esse inter se sociata, eorumque productum unitati aequivalere. Hoc nempe casu residua sociata sunt

$$\begin{array}{ccccc} 4, & -7, & -5, & 3, & -11, \\ 6, & -10, & 9, & 8, & 2. \end{array}$$

§ 39. Consideremus nunc quoque casus, quibus q est numerus compositus, ac primo quidem duplus cujuspiam numeri primi. Ab exemplo exordiamur quo $p = 13$ et $q = 6 = 2.3$, ac residua haec: 1, 4, −4, 3, −1, −3, unde hae quinque progressiones geometricae formentur:

I.	1,	4,	3,	−1,	−4,	−3,
II.	1,	−4,	3,	1,	−4,	3,
III.	1,	3,	−4,	1,	3,	−4,
IV.	1,	−1,	1,	−1,	1,	−1,
V.	1,	−3,	−4,	−1,	3,	4.

Ubi prima et quinta omnia continent residua; secunda vero et tertia eorum tantum semissem 1, −4, 3, quae bis repetuntur, reliquis, −1, +4, −3, exclusis: quarta vero duo tantum habet, +1 et −1, ter repetita. Similis ratio deprehenditur in casu $p = 29$ et $q = 14 = 2.7$, quo residua sunt: 1, −1, 4, −4, 5, −5, 6, −6, 7, −7, 9, −9, 13, −13, unde hae progressiones geometricae formantur:

I.	1,	−1,|	1,	−1,|	1,	−1,|	1,	−1,	1,	−1,|	1,	−1,|	1,	−1,
II.	1,	4,	−13,	6,	−5,	9,	7,	−1,	−4,	13,	−6,	5,	−9,	−7,
III.	1,	−4,	−13,	−6,	−5,	−9,	7,|	1,	−4,	−13,	−6,	−5,	−9,	7,
IV.	1,	5,	−4,	9,	−13,	−7,	−6,	−1,	−5,	4,	−9,	13,	7,	6,
V.	1,	−5,	−4,	−9,	−13,	7,	−6,|	1,	−5,	−4,	−9,	−13,	7,	−6,
VI.	1,	6,	7,	13,	−9,	4,	−5,	−1,	−6,	−7,	−13,	9,	−4,	5,
VII.	1,	−6,	7,	−13,	−9,	−4,	−5,|	1,	−6,	7,	−13,	−9,	−4,	−5,
VIII.	1,	7,	−9,	−5,	−6,	−13,	−4,|	1,	7,	−9,	−5,	−6,	−13,	−4,
IX.	1,	−7,	−9,	5,	−6,	13,	−4,	−1,	7,	9,	−5,	6,	−13,	4,

X. 1, 9, — 6, 4, 7, 5, —13, — 1, — 9, 6, — 4, — 7, — 5, 13,

XI. 1, — 9, — 6, — 4, 7, — 5, —13,| 1, — 9, — 6, — 4, 7, — 5, —13,

XII. 1, 13, — 5, — 7, — 4, 6, — 9, — 1, —13, 5, 7, 4, — 6, 9,

XIII. 1, —13, — 5, 7, — 4, — 6, — 9,| 1, —13, — 5, 7, — 4, — 6, — 9,

§ 40. Antequam hinc quicquam concludimus, evolvamus etiam casum, quo q est productum ex aliis binis numeris primis. Sit ergo divisor $p = 31$ et $q = 15 = 3.5$, quo casu residua sunt:

$$1, 4, 9, -15, -6, 5, -13, 2, -12, 7, -3, -11, 14, 10, 8$$

unde sequentes progressiones geometricae formantur, ubi quidem cuique suam sociatam retro dispositam adjungo:

{ I. 1, 4, —15, 2, 8,| 1, 4, —15, 2, 8,| 1, 4, —15, 2, 8,

{ II. 1, 8, 2, —15, 4,| 1, 8, 2, —15, 4,| 1, 8, 2, —15, 4,

{ III. 1, 9, —12, —15, —11, —6, 8, 10, — 3, 4, 5, 14, 2, —13, 7,

{ IV. 1, 7, —13, 2, 14, 5, 4, — 3, 10, 8, —6, —11, —15, —12, 9,

{ V. 1, 2, 4, 8, —15,| 1, 2, 4, 8, —15,| 1, 2, 4, 8, —15,

{ VI. 1, —15, 8, 4, 2,| 1, —15, 8, 4, 2,| 1, —15, 8, 4, 2,

{ VII. 1, — 3, 9, 4, —12, 5, —15, 14, —11, 2, —6, —13, 8, 7, 10,

{ VIII. 1, 10, 7, 8, —13, —6, 2, —11, 14, —15, 5, —12, 4, 9, — 3,

{ IX. 1, 5, — 6,| 1, 5, —6,| 1, 5, — 6,| 1, 5, — 6,| 1, 5, — 6,

{ X. 1, — 6, 5,| 1, — 6, 5,| 1, — 6, 5,| 1, —6, 5,| 1, — 6, 5,

{ XI. 1, —11, — 3, 2, 9, —6, 4, —13, —12, 8, 5, 7, —15, 10, 14,

{ XII. 1, 14, 10, —15, 7, 5, 8, —12, —13, 4, —6, 9, 2, — 3, —11,

{ XIII. 1, —12, —11, 8, — 3, 5, 2, 7, 9, —15, —6, 10, 4, 14, —13,

{ XIV. 1, —13, 14, 4, 10, —6, —15, 9, 7, 2, 5, — 3, 8. —11, —12,

§ 41. Has progressiones geometricas intuenti mox patet, earum alias esse completas, quarum termini omnia residua exibeant, alias vero esse periodicas, quae scilicet duabus pluribusve periodis constent, in quibus eadem residua eodem ordine recurrant, quam distinctionem inter progressiones completas et periodicas probe notasse juvabit. Periodicae scilicet locum inveniunt, quando, posito divisore primo $p = 2q + 1$, numerus q in duos factores est resolubilis, ut sit $q = mn$; tum enim ejusmodi progressiones geometricae dabuntur, quae continent m periodos, qualibet n residua complectentes; ac tales quidem assignari poterunt tot, quot numerus $n - 1$ continet unitates. Cum enim in eadem periodo cujusque termini omnes potestates occurrant, evidens est quemque, pro denominatore sumtum, similem progressionem periodicam producere, nisi forte periodorum numerus adeo duplicetur, vel multiplicetur, hoc est in duas pluresve periodos subdividatur.

§ 42. Ex progressione autem completa, quaecunque ea fit, facile reliquae omnes, sive sint completae, sive periodicae, formantur. Sit enim divisor primus $p = 2q + 1$, haecque progressio completa:

$$\begin{array}{lllllll} \text{Indices} & 0, & 1, & 2, & 3, & 4, & 5, \ldots\ldots q-1, \\ \text{Progr.} & 1, & \alpha, & \alpha^2, & \alpha^3, & \alpha^4, & \alpha^5 \ldots\ldots \alpha^{q-1}, \end{array}$$

si hinc excerpantur per saltus aequales termini:

$$\begin{array}{llllll} 0, & n, & 2n, & 3n, & 4n, & \ldots\ldots nq-n, \\ 1, & \alpha^n, & \alpha^{2n}, & \alpha^{3n}, & \alpha^{4n}, & \ldots\ldots \alpha^{nq-n}, \end{array}$$

haec progressio erit completa, si numerus n ad q fuerit primus; sin autem n et q habeant communem divisorem, puta d, tum haec progressio totidem habebit periodos, in quarum singulis eadem residua numero $\frac{q}{d}$ recurrent, reliqua autem inde prorsus excludentur. Numerus autem harum periodorum maximo communi divisore inter n et q definietur. At vero vicissim ex progressione periodica non licet progressionem completam formare.

§ 43. Imprimis autem hic notari meretur, in omnibus his progressionibus summam omnium terminorum semper esse nihilo aequalem, seu per divisorem p divisibilem, quod hoc modo demonstratur: Cum $\alpha^q - 1$ per p divisionem admittat, haec autem forma in factores resolvatur

$$\alpha - 1 \quad \text{et} \quad 1 + \alpha + \alpha^2 + \alpha^3 \ldots\ldots + \alpha^{q-1},$$

quorum ille $\alpha - 1$ certe non per p est divisibilis, necesse est hunc alterum, hoc est summam totius nostrae progressionis per numerum p divisionem admittere. Ac si progressio habeat periodos, termini cujusque periodi junctim sumti, seu summa omnium residuorum inde oriundorum per p erit divisibilis, id quod in exemplis supra allatis per se est manifestum.

§ 44. Ex eodem autem fonte colligitur, si progressio geometrica fuerit completa, et q habeat factorem m, ut sit $q = mn$ et divisor primus $p = 2mn + 1$, tum ob formam $\alpha^{mn} - 1$ divisibilem per $\alpha^m - 1$, quae per p divisibilis non existit, quia progressio alioquin completa non foret, quotum inde ortum:

$$1 + \alpha^m + \alpha^{2m} + \alpha^{3m} + \ldots\ldots + \alpha^{(n-1)m}$$

per divisorem p fore divisibilem. Quamobrem si tota progressio in membra distribuatur, hoc modo:

$$1, \alpha \ldots \alpha^{m-1} \mid \alpha^m + \alpha^{m+1} \ldots \alpha^{2m-1} \mid \alpha^{2m} + \alpha^{2m+1} \ldots \alpha^{3m-1} \mid \ldots \mid \alpha^{(n-1)m} \ldots \alpha^{mn-1},$$

quorum membrorum numerus est n, haecque membra ita sibi subscribantur:

$$\begin{array}{llll} 1, & \alpha, & \alpha^2 \ldots\ldots\ldots\ldots\ldots & \alpha^{m-1} \\ \alpha^m, & \alpha^{m+1}, & \alpha^{m+2} \ldots\ldots\ldots\ldots & \alpha^{2m-1} \\ \alpha^{2m}, & \alpha^{2m+1}, & \alpha^{2m+2} \ldots\ldots\ldots\ldots & \alpha^{3m-1} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \alpha^{(n-1)m}, & \alpha^{(n-1)m+1}, & \alpha^{(n-1)m+2} \ldots\ldots & \alpha^{nm-1} \end{array}$$

tum summae terminorum in qualibet columna verticali positorum ad nihilum reducentur, seu per divisorem primum $p = 2mn + 1$ divisibiles erunt. Tot autem diversis modis progressio completa in hujusmodi membra distribui potest, quot numerus q habuerit divisores.

§ 45. Prima autem columna verticalis simul dabit periodos pro omnibus progressionibus periodicis. De his numeris tenendum est, eos non solum esse residua quadratorum, sed etiam altiorum potestatum parium. Scilicet si divisor primus sit hujus formae: $p = 2mn + 1$, quemadmodum inter numeros ipso minores, quorum multitudo est $= 2mn$, tantum semissis mn in residuis quadratorum occurrit, totidemque inde excluduntur, ita potestates exponentis $2m$ per eundem numerum p dividendo, tantum n diversa residua inde resultant, et reliqui omnes, quorum multitudo est $(2m - 1)n$, ita sunt comparati, ut in forma $a^{2m} - ip$ nullo modo contineantur; seu nulla exhiberi possit potestas exponentis $2m$, quae ullo istorum numerorum minuta per numerum primum $p = 2mn + 1$ fiat divisibilis.

§ 46. Neque vero haec proprietas ad potestates exponentium parium est adstricta; sed in genere pronunciare licet, si divisor primus sit formae $p = mn + 1$, qui scilicet unitate minutus in factores m et n resolvi possit, ac potestates exponentis m, nempe

$$1,\ 2^m,\ 3^m,\ 4^m,\ 5^m,\ 6^m, \ldots\ldots (p-1)^m$$

per eum dividantur, tum inter residua tantum n diversos numeros occurrere, quorum singuli m vicibus repetantur; reliqui autem numeri omnes, quorum multitudo est $(m - 1)\,n$, hinc excludantur: ex quo insignes proprietates numerorum, qui sunt potestates, ratione divisibilitatis per numeros primos, agnoscere licet.

§ 47. Quoniam igitur nullum est dubium, quin hinc multae praeclarae numerorum proprietates erui queant, exempla plurium numerorum primorum hic adjicere visum est, pro iisque residua, quae ex divisione potestatum nascuntur, exhibere, ubi quidem sociata junctim repraesentantur:

1. Divisor $p = 3 = 2 + 1$

potest.	residuum
$a^2)$	1

2. divisor $p = 5 = 2.2 + 1$

potest.	residua
$a^2)$	1, -1
$a^4)$	1

3. divisor $p = 7 = 2.3 + 1$

potest.	residua
a^2	$\left\{1, \begin{matrix} 2 \\ -3 \end{matrix}\right\}$
$a^3)$	1, -1
$a^6)$	1

4. divisor $p = 11 = 2.5 + 1$

potest.	residua
a^2	$\left\{1, \begin{matrix} 4, & 5 \\ 3, & -2 \end{matrix}\right\}$
$a^5)$	1, -1
$a^{10})$	1

5. divisor $p = 13 = 2.2.3 + 1$

potest.	residua
a^2	$\left\{1, \begin{matrix} 4, & 3, \\ -3, & -4, \end{matrix} -1\right\}$
a^3	$\left\{1, \begin{matrix} -5, \\ 5, \end{matrix} -1\right\}$
a^4	$\left\{1, \begin{matrix} 3 \\ -4 \end{matrix}\right\}$
$a^6)$	1, -1
$a^{12})$	1

6. divisor $p = 17 = 2^4 + 1$

potest.	residua
a^2	$\left\{1, \begin{matrix} 2, & 4, & 8, \\ -8, & -4, & -2, \end{matrix} -1\right\}$
a^4	$\left\{1, \begin{matrix} 4, \\ -4, \end{matrix} -1\right\}$
$a^8)$	1, -1
$a^{16})$	1,

7. divisor $p = 19 = 2.3.3 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{cccc} 4, & -3, & 7, & 9 \\ 5, & 6, & -8, & -2 \end{array} \right\}$$

$$a^3 \left\{ 1, \begin{array}{cc} 8, & 7, \\ -7, & -8, \end{array} -1 \right\}$$

$$a^6 \left\{ 1, \begin{array}{c} 7 \\ -8 \end{array} \right\}$$

a^9) 1, -1

8. divisor $p = 23 = 2.11 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{ccccc} 4, & -7, & -5, & 3, & -11 \\ 6, & -10, & 9, & 8, & 2 \end{array} \right\}$$

a^{11}) 1, -1

9. divisor $p = 29 = 2.2.7 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{cccccc} 4, & -13, & 6, & -5, & 9, & 7, \\ -7, & -9, & 5, & -6, & 13, & -4, \end{array} -1 \right\}$$

$$a^4 \left\{ 1, \begin{array}{ccc} -13, & -5, & 7 \\ -9, & -6, & -4 \end{array} \right\}$$

$$a^7 \left\{ 1, \begin{array}{c} 12, \\ -12 \end{array} -1 \right\}$$

a^{14}) 1, -1

10. divisor $p = 31 = 2.3.5 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{ccccccc} 9, & -12, & -15, & -11, & -6, & 8, & 10 \\ 7, & -13, & 2, & 14, & 5, & 4, & -3 \end{array} \right\}$$

$$a^3 \left\{ 1, \begin{array}{cccc} -4, & -15, & -2, & 8, \\ -8, & 2, & 15, & 4, \end{array} -1 \right\}$$

$$a^5 \left\{ 1, \begin{array}{cc} -5, & -6, \\ 6, & 5, \end{array} -1 \right\}$$

$$a^6 \left\{ 1, \begin{array}{cc} 2, & 4 \\ -15, & 8 \end{array} \right\}$$

$$a^{10} \left\{ 1, \begin{array}{c} 5 \\ -6 \end{array} \right\}$$

a^{15}) 1, -1

11. divisor $p = 37 = 2.2.3.3 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{cccccccc} 4, & 16, & -10, & -3, & -12, & -11, & -7, & 9, \\ -9, & 7, & 11, & 12, & 3, & 10, & -16, & -4, \end{array} -1 \right\}$$

$$a^3 \left\{ 1, \begin{array}{ccccc} 8, & -10, & -6, & -11, & -14, \\ 14, & 11, & 6, & 10, & -8, \end{array} -1 \right\}$$

$$a^4 \left\{ 1, \begin{array}{cccc} 16, & -3, & -11, & 9 \\ 7, & 12, & 10, & -4 \end{array} \right\}$$

$$a^6 \left\{ 1, \begin{array}{cc} -10, & -11, \\ 11, & 10, \end{array} -1 \right\}$$

$$a^9 \left\{ 1, \begin{array}{c} -6, \\ 6, \end{array} -1 \right\}$$

$$a^{12} \left\{ 1, \begin{array}{c} -11 \\ 10 \end{array} \right\}$$

a^{18}) 1, -1

12. divisor $p = 41 = 2^3 . 5 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{rrrrrrrrr} -2, & 4, & -8, & 16, & 9, & -18, & -5, & 10, & -20, \\ 20, & -10, & 5, & 18, & -9, & -16, & 8, & -4, & 2, \end{array} -1 \right\}$$

$$a^4 \left\{ 1, \begin{array}{rrrr} 4, & 16, & -18, & 10, \\ -10, & 18, & -16, & -4, \end{array} -1 \right\}$$

$$a^5 \left\{ 1, \begin{array}{rrr} -3, & 9, & 14, \\ -14, & -9, & 3, \end{array} -1 \right\}$$

$$a^8 \left\{ 1, \begin{array}{rr} 16, & 10 \\ 18, & -4 \end{array} \right\}$$

$$a^{10} \left\{ 1, \begin{array}{r} 9, \\ -9, \end{array} -1 \right\}$$

$$a^{20}) \quad 1, -1$$

13. divisor $p = 43 = 2.3.7 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{rrrrrrrrrr} 9, & -5, & -2, & -18, & 10, & 4, & -7, & -20, & -8, & 14 \\ -19, & 17, & 21, & -12, & 13, & 11, & 6, & 15, & 16, & -3 \end{array} \right\}$$

$$a^3 \left\{ 1, \begin{array}{rrrrrr} 8, & 21, & -4, & 11, & 2, & 16, \\ -16, & -2, & -11, & 4, & -21, & -8, \end{array} -1 \right\}$$

$$a^6 \left\{ 1, \begin{array}{rrr} 21, & 11, & 16 \\ -2, & 4, & -8 \end{array} \right\}$$

$$a^7 \left\{ 1, \begin{array}{rr} -6, & -7, \\ 7, & 6, \end{array} -1 \right\}$$

$$a^{14} \left\{ 1, \begin{array}{r} -7 \\ 6 \end{array} \right\}$$

$$a^{21}) \quad 1, -1$$

14. divisor $p = 47 = 2.23 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{rrrrrrrrrrr} 4, & 16, & 17, & 21, & -10, & 7, & -19, & 18, & -22, & 6, & -23 \\ 12, & 3, & -11, & 9, & 14, & -20, & -5, & -13, & -15, & 8, & 2 \end{array} \right\}$$

$$a^{23}) \quad 1, -1$$

15. divisor $p = 53 = 2.2.13 + 1$

potest. residua

$$a^2 \left\{ 1, \begin{array}{rrrrrrrrrrrrr} 4, & 16, & 11, & -9, & 17, & 15, & 7, & -25, & 6, & 24, & -10, & 13, \\ -13, & 10, & -24, & -6, & 25, & -7, & -15, & -17, & 9, & -11, & -16, & -4, \end{array} -1 \right\}$$

$$a^4 \left\{ 1, \begin{array}{rrrrrr} 16, & -9, & 15, & -25, & 24, & 13 \\ 10, & -6, & -7, & -17, & -11, & -4 \end{array} \right\}$$

$$a^{13} \left\{ 1, \begin{array}{r} -23, \\ 23, \end{array} -1 \right\}$$

$$a^{26}) \quad 1, -1$$

16. divisor $p = 59 = 2.29 + 1$

potest.	residua															
a^2	1,	4,	16,	5,	20,	21,	25,	− 18,	− 13,	7,	28,	− 6,	− 24,	22,	29	
		15,	− 11,	12,	3,	− 14,	26,	− 23,	9,	17,	19,	− 10,	27,	− 8,	− 2	
a^{29}	1,	− 1														

17. divisor $p = 61 = 2.2.3.5 + 1$

potest.	residua															
a^2	1,	4,	16,	3,	12,	−13,	9,	−25,	22,	27,	−14,	5,	20,	19,	15,	−1
		−15,	− 19,	−20,	− 5,	14,	−27,	−22,	25,	− 9,	13,	−12,	− 3,	−16,	− 4,	
a^3	1,	8,	3,	24,	9,	11,	27,	−28,	20,	−23,	− 1					
		23,	−20,	28,	−27,	−11,	− 9,	−24,	− 3,	− 8,						
a^4	1,	16,	12,	9,	22,	−14,	20,	15								
		−19,	− 5,	−27,	25,	13,	− 3,	− 4								
a^5	1,	−29,	−13,	11,	−14,	−21,	− 1									
		21,	14,	−11,	13,	29,										
a^6	1,	3,	9,	27,	20,	− 1										
		−20,	−27,	− 9,	− 3,											
a^{10}	1,	−13,	−14,	− 1												
		14,	13,													
a^{12}	1,	− 3,	9													
		20,	−27													
a^{15}	1,	11,	− 1													
		−11,														
a^{20}	1,	−14														
		13														
a^{30}	1,	− 1.														

Conclusio.

De potestatibus cujusque ordinis et residuis, in earum divisione per numeros primos relictis.

§ 48. Quemadmodum in his exemplis residua pro singulis potestatibus per progressiones geometricas sunt exhibita, quae simul retro continuatae bina residua sociata junctim repraesentant, ita idem pro potestatibus primi ordinis fieri potest, ubi quidem omnes plane numeri divisore minores occurrere debent, ita ut si divisor primus sit $p = 2q + 1$, multitudo residuorum diversorum sit $= 2q$, quae ad minimam formam reducta erunt ± 1, ± 2, ± 3, ± 4, etc. usque ad $\pm q$. Haec vero residua omnia quoque secundum progressionem geometricam disponi possunt, ab unitate incipientem, dummodo pro ejus denominatore, seu secundo termino ejusmodi numerus accipiatur, qui omnes plane numeros producat, quod evenit, si is ita fuerit comparatus, ut nulla ejus potestas, cujus exponens minor sit quam $2q$, pro residuo unitatem relinquat. Tales autem numeros pro

quovis divisore dari certum est, etiamsi eos assignare maxime difficile videatur, eorumque indoles ad profundissima numerorum mysteria sit referenda.

§ 49. Sit igitur in genere pro divisore primo $p = 2q + 1$, littera a ejusmodi numerus, cujus potestates per p divisae omnes numeros ipso p minores pro residuis relinquant; neque in serie geometrica $1, a, a^2, a^3, a^4$, etc. unitas ante recurrat, quam ad potestatem a^{2q} fuerit perventum, quippe quae semper per $p = 2q + 1$ divisa unitatem relinquit, sicque omnes potestates hac minores diversa residua producant. Cum igitur potestas a^q non relinquat unitatem, et $a^{2q} - 1 = (a^q + 1)(a^q - 1)$ per numerum p divisionem admittat, erit $a^q + 1$ per p divisibilis, et potestas a^q residuum dabit $- 1$; tum vero sequentes potestates $a^{q+1}, a^{q+2}, a^{q+3}$, etc. dabunt residua $-a, -a^2, -a^3$, etc. quae ita sunt comparata, ut cum antecedentibus $a^{q-1}, a^{q-2}, a^{q-3}$, etc. ordine juncta bina residua sociata exhibeant, quorum scilicet productum a^{2q} unitati aequivaleat. Sequenti ergo modo haec residua per associationem repraesentare poterimus:

indices	0,	1,	2,	3.	4, . .	$q-3$,	$q-2$,	$q-1$,	q
	1,	a^1,	a^2,	a^3,	a^4, . .	a^{q-3},	a^{q-2},	a^{q-1},	-1
		$-a^{q-1}$,	$-a^{q-2}$,	$-a^{q-3}$,	$-a^{q-4}$, . .	$-a^3$,	$-a^2$,	$-a$,	
indices	$2q$,	$2q-1$,	$2q-2$,	$2q-3$,	$2q-4$, . .	$q+3$,	$q+2$,	$q+1$,	q

ubi bina residua sibi subscripta sunt inter se sociata, extrema vero $+1$ et -1 solitaria, quippe quae secum ipsa sociantur.

§ 50. Tali progressione geometrica constituta, quae omnia residua ex potestatibus primi ordinis oriunda, hoc est omnes plane numeros complectitur, ex ea omnia residua pro potestatibus cujusvis ordinis innotescent, eodem scilicet divisore primo $p = 2q + 1$ retento. Residua nimirum ex divisione quadratorum orta erunt:

$$1,\ a^2,\ a^4,\ a^6,\ a^8,\ \text{etc.} \ldots\ldots a^{2q-2},$$

quae indicibus tantum paribus respondent, et ita per associationem exhibentur:

$$1,\ \begin{matrix} a^2, & a^4, & a^6, & a^8, \\ -a^{q-2}, & -a^{q-4}, & -a^{q-6}, & -a^{q-8}, \end{matrix}\ \text{etc.}$$

in quibus ergo -1 reperietur, si q fuerit numerus par. Pro cubis autem eos tantum terminos accipi oportet, quorum indices sunt multipla ternarii $1, a^3, a^6, a^9$, etc. Unde patet, si exponens $2q$ divisionem per 3 admittat, multitudinem residuorum ad trientem redigi, dum reliquis casibus omnia plane residua occurrunt. Simili modo residua potestatum quartarum obtinentur ex indicibus per 4 divisibilibus, seu ex his potestatibus: $1, a^4, a^8, a^{12}$, etc. et residua potestatum quintarum ex his: $1, a^5, a^{10}, a^{15}$, etc.

§ 51. Tantum ergo opus est, ut pro quolibet divisore primo $p = 2q + 1$ idonei numeri pro a habeantur, ex cujus potestatibus omnia plane residua resultent; ad quod autem nullam certam regulam mihi esse cognitam fateri cogor. Hoc saltem observasse juvabit, si unus hujusmodi numerus a fuerit cognitus, ejus socium, qui sit b, ut $ab - 1$ per p fiat divisibile, quoque pari proprietate esse praeditum: vidimus autem hunc socium b vel per a^{2q-1}, vel per $-a^{q-1}$ exhiberi posse. Ex quo concludere licet, tum etiam pro a quamvis ejus potestatem a^n, cujus exponens n sit ad nume-

rum $2q$ primus, accipi posse, ubi quidem sufficit pro n numeros ipso $2q$ minores assumsisse, cum ex altioribus potestatibus eadem residua repetantur. Quoniam vero certa lex adhuc latet, pro divisoribus simplicioribus idoneos numeros pro a assumendos, ex cujus scilicet potestatibus omnia plane residua nascantur, exhibebo:

Divis. primi	Numeri pro a assumendi
$p = 3$, $q = 1$	-1
$p = 5$, $q = 2$	$+2, -2$
$p = 7$, $q = 3$	$-2, +3$
$p = 11$, $q = 5$	$+2, -3, -4, -5$
$p = 13$, $q = 6$	$+2, -2, +6, -6$
$p = 17$, $q = 8$	$+3, -3, +5, -5, +6, -6, +7, -7$
$p = 19$, $q = 9$	$+2, +3, -4, -5, -6, -9$
$p = 23$, $q = 11$	$-2, -3, -4, +5, -6, +7, -8, -9, +10, +11$
$p = 29$, $q = 14$	$+2, -2, +3, -3, +8, -8, +10, -10, +11, -11, +14, -14$
$p = 31$, $q = 15$	$+3, -7, -9, -10, +11, +12, +13, -14$
$p = 37$, $q = 18$	$+2, -2, +5, -5, +13, -13, +15, -15, +17, -17, +18, -18$
$p = 41$, $q = 20$	$\pm 6, \pm 7, \pm 11, \pm 12, \pm 13, \pm 15, \pm 17, \pm 19.$

§ 52. In casu postremo $p = 41$ ergo patet, pro a minorem numerum quam 6 assumi non posse, cum in praecedentibus progressio geometrica ex minoribus numeris formari queat: unde pro hoc divisore $p = 41$ ista progressio geometrica ita se habebit:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1,	+6,	−5,	+11,	−16,	−14,	−2,	−12,	+10,	+19,	−9,	−13,	+4,	−17,	−20,	+3,	+18,	−15,	−8,	−7,	−1
	+7,	+8,	+15,	−18,	−3,	+20,	+17,	−4,	+13,	+9,	−19,	−10,	+12,	+2,	+14,	+16,	−11,	+5,	−6,	

Hinc si ii numeri excerpantur, qui indicibus paribus respondent, habebuntur residua ex quadratis orta: sin autem ii excerpantur, qui indicibus vel per 4, vel 5, vel 8, vel 10, vel 20 conveniunt, residua pro ejusdem nominis potestatibus obtinebuntur, eaque ipsa, quae jam supra sunt recensita. Similisque est ratio omnium reliquorum numerorum primorum.

§ 53. Quod autem ad multitudinem horum numerorum a attinet, observo eam quovis casu $p = 2q + 1$ aequalem esse multitudini eorum numerorum ipso p minorum, qui sint ad $2q$ primi: atque alio loco ostendi, ad hanc multitudinem inveniendam numerum $2q$ in factores suos primos resolvi debere, ita ut si fuerit $2q = f^{\lambda} g^{\mu} h^{\nu} k^{\kappa}$, sit ista multitudo

$$= (f-1) f^{\lambda-1} . (g-1) g^{\mu-1} . (h-1) h^{\nu-1} . (k-1) k^{\kappa-1}.$$

Definito autem pro quovis numero $p = 2q + 1$ hac multitudine, sint ipsi numeri ad $2q$ primi $1, \alpha, \beta, \gamma, \delta$, etc. atque si datus fuerit unus numerus a quicunque, reliqui ideoque omnes erunt:

$$a, \quad a^{\alpha} - np, \quad a^{\beta} - np. \quad a^{\gamma} - np, \quad a^{\delta} - np, \quad \text{etc.}$$

sumendo n ita, ut omnes isti numeri infra p deprimantur. Haec fortasse consideratio viam aperiet pro quovis casu hos numeros investigandi.

XXXVI.

Solutio problematis de inveniendo triangulo in quo rectae ex singulis angulis latera opposita bisecantes sint rationales.

(N. Comment. XVIII. 1773. p. 171. Exhib. 1772 Aug. 24.)

1. Vocatis ternis lateribus $2a$, $2b$, $2c$ et rectis haec latera bisecantibus f, g, h: quaestio reducitur ad resolutionem trium sequentium formularum

$$2bb + 2cc - aa = ff,$$
$$2cc + 2aa - bb = gg,$$
$$2aa + 2bb - cc = hh.$$

2. Hinc differentiis sumendis sequitur fore:

$$3(bb - aa) = ff - gg, \quad 3(cc - bb) = gg - hh, \quad 3(cc - aa) = ff - hh,$$

seu

$$ff + 3aa = gg + 3bb = hh + 3cc.$$

Cum autem sit $ff = 2bb + 2cc - aa$, habebimus,

$$ff + 3aa = gg + 3bb = hh + 3cc = 2(aa + bb + cc).$$

3. Summa porro nostrarum trium formularum praebet:

$$2(ff + gg + hh) = 3ff + 9aa = 3gg + 9bb = 3hh + 9cc$$

ita ut hinc istae ternae formulae resultent:

$$2gg + 2hh - ff = 9aa,$$
$$2hh + 2ff - gg = 9bb,$$
$$2ff + 2gg - hh = 9cc.$$

4. Quae cum similes sint ipsis propositis, concludimus si pro lateribus $2a$, $2b$, $2c$ sint rectae bisecantes f, g, h, tum pro lateribus $2f$, $2g$, $2h$ fore rectas bisecantes $3a$, $3b$, $3c$, ideoque pro lateribus f, g, h rectas bisecantes $\frac{3}{2}a$, $\frac{3}{2}b$, $\frac{3}{2}c$. Quare invento uno hujusmodi triangulo, si rectae bisecantes pro lateribus novi trianguli accipiantur, hoc eadem gaudebit proprietate, quia in hoc rectae bisecantes sunt tres quadrantes laterum praecedentis.

5. His observatis solutionem quaestionis sequenti modo aggredior. Primo binis tantum formulis satisfacturus eas ita exhibeo:

$$(b - c)^2 + (b + c)^2 - aa = (b - c)^2 + (b + c + a)(b + c - a) = ff,$$
$$(a - c)^2 + (a + c)^2 - bb = (a - c)^2 + (a + c + b)(a + c - b) = gg.$$

Statuo igitur:

$$f = b - c + (b + c + a)p \quad \text{et} \quad g = a - c + (a + c + b)q,$$

ut facta substitutione divisio per $a+b+c$ succedat, hoc modo obtinetur:

$$b+c-a=2(b-c)p+(b+c+a)pp,$$
$$a+c-b=2(a-c)q+(a+c+b)qq.$$

6. Ex utraque aequatione definiatur valor ipsius c:

$$c=\frac{a(1+pp)-b(1-2p-pp)}{1+2p-pp}=\frac{b(1+qq)-a(1-2q-qq)}{1+2q-qq}$$

unde fit

$$a+b+c=\frac{2a(1+p)+4bp}{1+2p-pp}=\frac{2b(1+q)+4aq}{1+2q-qq},$$

ex quo duplici valore ratio inter numeros a et b colligitur:

$$a(1+p)(1+2q-qq)-2aq(1+2p-pp)=b(1+q)(1+2p-pp)-2bp(1+2q-qq),$$

quamobrem statuo:

$$a=1+q-pp-2pq-ppq+2pqq,$$
$$b=1+p-qq-2pq-pqq+2ppq,$$

hincque fit

$$\frac{a+b+c}{2}=\frac{1+3p+q+pp-pq-7ppq-p^3+3p^3q}{1+2p-pp}$$

seu

$$a+b+c=2+2p+2q-6pq.$$

7. Cum igitur sit:

$$a+b=2+p+q-pp-qq-4pq+ppq+pqq,$$

erit

$$c=p+q+pp+qq-2pq-ppq-pqq;$$

sicque binis formulis satisfit, numeris a, b, c sequentes valores tribuendo:

$$a=1+q-pp-2pq-ppq+2pqq,$$
$$b=1+p-qq-2pq-pqq+2ppq,$$
$$c=p+q+pp+qq-2pq-ppq-pqq,$$

unde cum fiat

$$a+b+c=2+2p+2q-6pq,$$
$$b-c=1-q-pp-2qq+3ppq,$$
$$a-c=1-p-qq-2pp+3pqq,$$

habebimus:

$$f=1+2p-q+pp-2qq+2pq-3ppq \quad \text{et} \quad b-c+f=2(1+q)(1+q-2q)$$
$$g=1+2q-p+qq-2pp+2pq-3pqq \qquad\quad a-c+g=2(1+p)(1+q-2p).$$

8. Juvabit hinc etiam sequentes valores elicuisse:

$$a+b-c=2-2pp-2qq-2pq+2ppq+2pqq=2(1-p)(1-q)(1+p+q)$$
$$b+c-a=2p+2pp-2pq-4pqq+2ppq=2p(1+q)(1+p-2q)$$
$$a+c-b=2q+2qq-2pq-4ppq+2pqq=2q(1+p)(1+q-2p),$$

ubi cavendum est, ne harum ulla evanescat, quia alioquin triangulum periret; excluduntur ergo sequentes valores:

$$p=0,\quad q=0,\quad p=\pm 1,\quad q=\pm 1,\quad p+q=-1,\quad q=\frac{p+1}{2},\quad p=\frac{q+1}{2}.$$

Praeterea vero etiam excludi oportet $1+p+q=3pq$, ne summa laterum evanescat. Tum vero etiam notetur esse:

$$a-b=q+p+qq-pp+3pqq-3ppq=(q-p)(1+p+q+3pq),$$
$$g-f=3q-3p+3qq-3pp-3pqq+3ppq=3(q-p)(1+p+q-pq)$$

tandem vero est

$$aa+bb+cc=2(1-p-q+pp-pq+qq)(1+2(p+q)+(p+q)^2+3ppqq)$$

seu

$$aa+bb+cc=\tfrac{1}{2}((2-p-q)^2+3(p-q)^2)((1+p+q)^2+3ppqq).$$

9. Superest igitur ut tertia conditio impleatur, quae in hac formula continetur:

$$hh=(a+b)^2+(a-b)^2-cc=(a-b)^2+(a+b+c)(a+b-c),$$

ubi si valores modo indicati substituantur, colligitur:

$$hh=(q-p)^2(1+p+q+3pq)^2+4(1-p)(1-q)(1+p+q)(1+p+q-3pq)$$

quae evolvitur in hanc formam:

$$hh=9ppqq(q-p)^2+6pq(p+q)(pp-4pq+qq)+p^4+22p^3q+6ppqq+22pq^3+q^4$$
$$-2(p+q)^3-3(pp+6qq)+4(p+q)+4,$$

quae secundum potestates ipsius q disposita fit

$$hh=(1+3p)^2q^4-2(1-11p+9pp+9p^3)q^3-3(1+2p-2pp+6p^3-3p^4)q^2$$
$$+2(2-9p-3pp+11p^3+3p^4)q+(2+p-pp)^2.$$

10. Alia methodus hanc aequationem resolvendi non patet, nisi ut more solito pro h ejusmodi expressio assumatur, qua substituta valor ipsius q per aequationem simplicem determinetur. Tum vero constat, quomodo uno valore invento, ex eo continuo plures elici queant. Ad minores autem valores eruendos, generatim notetur, si fuerit

$$hh=AAq^4+2Bq^3+Cqq+2Dq+EE$$

sequentibus positionibus negotium confectum iri:

1. si $h=Aqq+\frac{B}{A}q\pm E$, fit $\quad q=\frac{2A(AD\mp BE)}{BB-AA(C\mp 2AE)}$,

2. si $h=\pm Aqq+\frac{D}{E}q+E$, fit $\quad q=\frac{DD-EE(C\mp 2AE)}{2E(BE\mp AD)}$,

3. si $h=Aqq+\frac{B}{A}q+\frac{C}{2A}-\frac{BB}{2A^3}$, fit $\quad q=\frac{(BB-AAC)^2-4A^4EE}{4BA(B(BB-AAC)+2A^4D)}$,

4. si $h=\frac{CEE-DD}{2E^3}qq+\frac{D}{E}q+E$, erit $\quad q=\frac{4EE(D(DD-CEE)+2BE^4)}{(DD-CEE)^2-4AAE^4}$.

11. Cum autem casus supra exclusi nostrae aequationi sponte satisfaciant, et pro hh quadratum producant, ex iis novas formas similes elicere licet, unde deinceps novi valores idonei pro q erui queant. Sit ergo primo $q=1+x$ eritque

$$hh=(1-p+x)^2(2+4p+(1+3p)x)^2-4x(1-p)(2+p+x)(2-2p+(1-3p)x),$$

quae evoluta praebet hanc formam:

$$hh = (1+3p)^2x^4 + 2(1+23p+9pp-9p^3)x^3 + (-3+92p+10pp-72p^3+9p^4)xx$$
$$+ 4(1-p)(-1+12p+10pp-6p^3)x + 4(1-p)^2(1+2p)^2$$

tum vero est

$$a+b-c = -2x(1-p)(2+p+x),$$
$$b+c-a = -2p(2+x)(1-p+2x),$$
$$a+c-b = 2(1+p)(1+x)(2-2p+x).$$

Praestabit autem quovis casu, quo loco p determinatus valor assumitur, substitutionem in priori forma facere, ac tum denique evolutionem instituere.

12. Sit igitur secundo $q = -1-p+x$, eritque

$$hh = (1+2p-x)^2(3p(1+p)-(1+3p)x)^2 + 4x(1-p)(2+p-x)(3p(1+p)+(1-3p)x)$$

atque

$$a+b-c = 2x(1-p)(2+p-x),$$
$$b+c-a = -2p(p-x)(3+3p-2x),$$
$$a+c-b = 2(1+p)(1+p-x)(3p-x).$$

Sit tertio $q = -1+x$ eritque

$$hh = (1+p-x)^2(2p-(1+3p)x)^2 + 4(1-p)(2-x)(p+x)(4p+(1-3p)x)$$

atque

$$a+b-c = 2(1-p)(2-x)(p+x),$$
$$b+c-a = 2px(3+p-2x)$$
$$a+c-b = 2(1+p)(1-x)(2p-x).$$

Sit quarto $q = \frac{1+p+x}{2}$ eritque

$$16hh = (1-p+x)^2(3(1+p)^2+(1+3p)x)^2 + 8(1-p)(1-p-x)(3+3p+x)(3(1-pp)+(1-3p)x)$$

atque

$$a+b-c = \tfrac{1}{2}(1-p)(1-p-x)(3(1+p)+x),$$
$$b+c-a = -px(3+p+x),$$
$$a+c-b = \tfrac{1}{2}(1+p)(1+p+x)(3(1-p)+x).$$

Sit denique quinto $q = \frac{1+p+x}{3p-1}$, erit

$$(3p-1)^4hh = ((1-p)(1+3p)+x)^2(6p(1+p)+(1+3p)x)^2$$
$$+ 4(3p-1)^2x(1-p)(2(1-p)+x)(3p(1+p)+x)$$

atque

$$a+b-c = \frac{-2(1-p)(2(1-p)+x)(3p(1+p)+x)}{(3p-1)^2},$$
$$b+c-a = \frac{-2p(4p+x)(3(1-pp)+2x)}{(3p-1)^2},$$
$$a+c-b = \frac{2(1+p)(1+p+x)(6p(1-p)+x)}{(3p-1)^2},$$

semper autem est

$$f = b-c+(a+b+c)p \quad \text{et} \quad g = a-c+(a+b+c)q.$$

13. Hinc ergo satis patet innumerabiles solutiones nostri problematis inveniri posse. Invento enim pro q valore quocunque $q = n$, statuatur $q = n + x$, et aequatio resultans iterum hujusmodi formam habebit

$$hh = AAx^4 + 2Bx^3 + Cxx + 2Dx + EE$$

unde novos valores pro x et h eruere licet methodo ante indicata. Cum autem hic potissimum solutiones in minoribus numeris desiderentur, litterae p valores simpliciores tribuamus, unde quidem valores 0 et ± 1 excludi conveniet.

Casus 1. $p = -2$.

14. Ob $p = -2$, habemus:

$$a = -3 + q - 4qq, \quad f = 1 - 17q - 2qq,$$
$$b = -1 + 12q + qq, \quad g = -5 - 2q + 7qq,$$
$$c = \quad 2 + q + 3qq, \quad a + b + c = -2 + 14q$$

unde fieri oportet

$$hh = (q + 2)^2 (5q + 1)^2 - 12 (q - 1)^2 (7q - 1),$$

quae evoluta abit in hanc formam:

$$25q^4 + 26q^3 + 321qq - 64q + 16 = hh.$$

Hic igitur est $A = 5$, $B = 13$, $C = 321$, $D = -32$ et $E = 4$, ideoque sequentes solutiones nascuntur;

$$1.\ \text{si}\ h = 5qq + \tfrac{13}{5}q \pm 4, \quad \text{fit}\ q = \frac{10(40 \pm 13)}{1964 \mp 250},$$

$$2.\ \text{si}\ h = \pm 5qq - 8q + 4, \quad \text{fit}\ q = \frac{-257 \pm 40}{26 \pm 80},$$

ubi tertiam et quartam, quia numeros nimis magnos praebent, omitto.

15. Prioris solutionis signum superius praebet:

$$q = \frac{10.53}{1714} = \frac{5.53}{857},$$

unde nascuntur numeri nimis magni; signum vero inferius

$$q = \frac{10.27}{2214} = \frac{15}{123} = \frac{5}{41}, \quad \text{ergo} \quad h = \frac{-6066}{1641}.$$

Posterioris vero solutionis signum superius dat

$$q = \frac{-217}{105},$$

signum vero inferius:

$$q = \frac{-297}{-54} = \frac{11}{2}, \quad \text{ergo} \quad h = \frac{765}{4},$$

unde etiam reliquas litteras definiamus

$$a = -\frac{237}{2}, \quad b = \frac{381}{4}, \quad c = \frac{393}{4},$$
$$f = -153, \quad g = \frac{783}{4}, \quad h = \frac{765}{4}.$$

Hos numeros multiplicemus per 4 ac dividamus per 3, ut obtineamus hanc solutionem satis simplicem:

$$a = 158,\quad b = 127,\quad c = 131,$$
$$f = 204,\quad g = 261,\quad h = 255,$$

et quia litterae f, g, h, quae communem habent divisorem 3, in locum litterarum a, b, c substitui possunt, prodibit haec solutio multo simplicior

$$a = 69,\quad b = 87,\quad c = 85,$$
$$f = 158,\quad g = 127,\quad h = 131,$$

unde fit $aa + bb + cc = 2.7.19.73$, qui factores utique sunt numeri formae $xx + 3yy$, uti natura rei postulat.

16. Cum loco q satisfaciat tam $+1$ quam -1, utamur hac substitutione $q = \frac{y+1}{y-1}$ fietque

$$\tfrac{1}{4}(y-1)^4 hh = 81y^4 + 54y^3 - 99yy - 36y + 100$$

unde ob

$$A = 9,\quad B = 27,\quad C = -99,\quad D = -18,\quad E = 10,$$

habebimus has resolutiones:

1. si $\frac{1}{2}(y-1)^2 h = 9yy + 3y \pm 10$, erit $y = \frac{-9(3 \pm 5)}{27(3 \pm 5)} = -\frac{1}{3}$,

2. si $\frac{1}{2}(y-1)^2 h = \pm 9yy - \frac{9}{2}y + 10$, erit $y = \frac{9 + 25(11 \pm 20)}{30(5 \pm 3)}$,

quarum prior dat $q = -\frac{1}{2}$, qui est casus exclusus forma $q = \frac{p+1}{2}$; altera vero suppeditat

$$\text{sub signo superiori}\quad y = \frac{784}{240} = \frac{49}{15} \quad\text{et}\quad q = \frac{32}{17},$$
$$\text{sub signo inferiori}\quad y = \frac{-24.9}{60} = \frac{-18}{5} \quad\text{et}\quad q = \frac{13}{23}.$$

17. Sit ergo $y = \frac{49}{15}$ et $q = \frac{32}{17}$ eritque

$$\frac{2.17^2}{15^2} h = \frac{2504}{25} \quad\text{hinc}\quad h = \frac{9.1252}{289},$$

porro

$$a = -3 + \frac{32}{17} - \frac{4096}{289} = -\frac{4419}{289},$$
$$b = -1 + \frac{12.32}{17} + \frac{1024}{289} = \frac{7263}{289},$$
$$c = 2 + \frac{32}{17} + \frac{3072}{289} = \frac{4194}{289},$$
$$f = 1 - \frac{17.32}{17} - \frac{2048}{289} = -\frac{11007}{289},$$
$$g = -5 - \frac{2.32}{17} + \frac{7.1024}{289} = \frac{4635}{289}.$$

Omnes hi valores per 289 multiplicati per 9 deprimantur, et habebitur ista solutio

$$a = 491,\quad b = 807,\quad c = 466,$$
$$f = 1223,\quad g = 515,\quad h = 1252,$$

quae eadem resultat ex altero casu invento $q = \frac{13}{23}$, unde est $aa + bb + cc = 2.7.19.43.97$.

Casus 2. $p=2$.

18. Pro hoc ergo casu primo habemus:

$$a+b-c=-2(1-q)(3+q),\quad b-c+f=\frac{b+c-a}{2},$$
$$b+c-a=4(1+q)(3-2q),\quad a-c+g=\frac{a+c-b}{q},$$
$$a+c-b=-6q(3-q),$$

unde fit

$$hh=(q-2)^2(7q+3)^2-4(1-q)(3+q)(3-5q),$$

quae evoluta praebet hanc formam:

$$hh=49q^4-174q^3+9qq+216q$$

haecque facto $q=3r$ transit in hanc simpliciorem

$$\frac{1}{81}hh=49r^4-58r^3+rr+8r,$$

casus autem excludendi sunt $q=\pm 1$, $q=-3$, $q=\frac{3}{2}$, $q=3$ et $q=\frac{3}{5}$.

19. Cum hic sit $A=7$, $B=-29$, $C=1$, $D=4$, $E=0$, erit ex solutione prima, sumto $\frac{1}{9}\cdot h=7rr-\frac{29}{7}r$,

$$r=\frac{14.28}{841-49}=\frac{49}{99}\quad\text{et}\quad q=\frac{49}{33},\ \text{hincque}\quad h=-\frac{7.470}{11.99}$$

tum vero porro

$$a+b-c=\frac{2.16.148}{33.33},\qquad b-c+f=\frac{4.41}{33.33},$$
$$b+c-a=\frac{4.82.1}{33.33},\qquad a-c+g=-\frac{6.50}{33},$$
$$a+c-b=-\frac{6.49.50}{33.33},$$

multiplicentur hi valores omnes per $\frac{33.33}{4}$, erit

$$\begin{array}{lll} a+b-c=\ \ 1184, & 2c=-3593, & 2f=-4777,\\ b+c-a=\ \ \ \ 82, & 2a=-2491, & 2g=-6092,\\ a+c-b=-3675, & 2b=+1266, & 2h=-1645.\\ a+b+c=-2409, & & \end{array}$$

Duplicatis ergo valoribus prodit haec solutio

$$a=2491,\quad b=1266,\quad c=3593,$$
$$f=4777,\quad g=6092,\quad h=1645,$$

hinc vero est $aa+bb+cc=2.19.31.43.409$.

20. Transformemus aequationem nostram ponendo $r=\frac{y+1}{y-1}$, orieturque

$$\frac{1}{324}hh(y-1)^4=25+82y+73yy+16y^3;$$

statuatur $\frac{1}{18}h(y-1)^2=5+\frac{41}{5}y$, fitque $y=-\frac{9}{25}$, hinc

$$r = -\frac{8}{17} \quad \text{et} \quad q = -\frac{24}{17}; \quad \text{ideoque} \quad h = \frac{45.128}{289};$$

porro

$$a+b-c = -\frac{2.41.27}{289}, \quad b-c+f = -\frac{2.7.99}{289},$$

$$b+c-a = -\frac{4.7.99}{289}, \quad a-c+g = -\frac{6.17.75}{289},$$

$$a+c-b = \frac{6.24.75}{289}.$$

Multiplicentur omnes hi valores per $\frac{289}{9}$ et habebitur

$$a+b-c = -246, \quad 2c = 892, \quad h = 640,$$
$$b+c-a = -308, \quad 2a = 954, \quad b-c+f = -154, \quad f = 569,$$
$$a+c-b = 1200, \quad 2b = -554, \quad a-c+g = -850, \quad g = -881,$$
$$a+b+c = 646,$$

unde colligitur haec solutio:

$$a = 477, \quad b = 277, \quad c = 446,$$
$$f = 569, \quad g = 881, \quad h = 640.$$

21. In aequatione per q expressa statuatur $q = \frac{y+1}{y-1}$, ac reperietur

$$\tfrac{1}{4} hh (y-1)^4 = 25y^4 - 146y^3 + 69yy + 244y + 4,$$

ubi $A = 5$, $B = -73$, $C = 69$, $D = 122$, $E = 2$. Ergo

1. si $\frac{1}{2} h (y-1)^2 = 5yy - \frac{73}{5} y \pm 2$, fit

$$y = \frac{10(610 \pm 146)}{73^2 - 25(69 \mp 20)} = \frac{5(305 \pm 73)}{901 \pm 125},$$

2. si $\frac{1}{2} h (y-1)^2 = 5yy + 61y + 2$, fit

$$y = \frac{4.61^2 - 4(69 \mp 20)}{4(-146 \mp 610)} = \frac{1826 \pm 10}{-73 \mp 305}.$$

Ex priori dat signum superior $y = \frac{5.378}{1026} = \frac{35}{19}$ et $q = \frac{27}{8}$, at signum inferior $y = \frac{5.232}{776} = \frac{145}{97}$ et $q = \frac{121}{24}$. Ex secunda dat signum superior $y = \frac{1836}{-378} = -\frac{34}{7}$ et $q = \frac{27}{41}$, at signum inferior $y = \frac{1816}{232} = \frac{227}{29}$ et $q = \frac{128}{99}$.

Ex valore $q = \frac{27}{8}$ colligimus hanc solutionem

$$a = 404, \quad b = 377, \quad c = 619,$$
$$f = 3.314, \quad g = 3.325, \quad h = 3.159,$$

ubi fit $aa + bb + cc = 2.3.7.13^2.97$.

Ex valore autem $q = \frac{27}{41}$ nascitur ista solutio

$$a = 134, \quad b = 823, \quad c = 607,$$
$$f = 3.480, \quad g = 3.103, \quad h = 3.337,$$

ubi est $aa + bb + cc = 2.3.7.19.31.43$ notandumque est hic bina latera tertio non esse majora.

22. Pluribus casibus evolvendis hic non immoror, sed potius animadverto, methodum qua hic sum usus, non satis videri naturalem et ad scopum accommodatam, propterea quod nulla suppeditat criteria solutiones simpliciores distinguendi. Desideratur ergo tam pro hoc problemate, quam pro aliis similibus, quorum solutio ad hujusmodi formam

$$Ax^4 + Bx^3 + Cx^2 + Dx + E$$

ad quadratum reducendam, revocatur. Atque in hoc quidem problemate solutio a quantitate $aa + bb + cc$ inchoanda videtur, quae hujusmodi numero $2(xx + 3yy)$ certe est aequalis; et cum debeat esse

$$4(xx + 3yy) = ff + 3aa = gg + 3bb = hh + 3cc,$$

evidens est numerum $xx + 3yy$ factores habere debere, quos constat ejusdem esse formae. Statui igitur poterit

$$xx + 3yy = (mm + 3nn)(pp + 3qq)(rr + 3ss)$$

et $4(xx + 3yy)$ octo modis ad formam $AA + 3BB$ referri potest, unde ternas illas eligi oportet. Foret nempe

$$a = 2m(ps + qr) + 2n(3qs - pr),$$
$$b = m((3q + p)s \pm (q - p)r) \pm n(3(q - p)s \mp (3q + p)r),$$
$$c = n((3q - p)s \pm (q + p)r) \pm n(3(q + p)s \mp (3q - p)r),$$

et effici restat

$$aa + bb + cc = 4(xx + 3yy).$$

Verum hoc modo calculus fit satis prolixus, nisi forte certis artificiis tractabilior reddi potest.



XXXVII.

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia.

(N. Comment. XVIII. 1773. p. 85. Exhib. 1772 Maj. 18.)

1. **Hypothesis.** Si termini progressionis geometricae ab unitate incipientis per numerum primum P dividantur, residua inde nata litteris 1, α, β, γ, δ, etc. denotabo, hoc modo:

Progr. geom.	$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6$ etc.
Residua	$1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta$ etc.

Conclusiones.

2. Omnia haec residua sunt minora divisore P; quamdiu enim termini progressionis geometricae divisore P sunt minores, residua ipsis sunt aequalia; cum autem divisorem P superant, auferendo ab iis divisorem P, quoties fieri potest, residua tandem ipso P minora relinqui necesse est.

3. Si numerus a sit primus ad divisorem P, hoc est si neque ipsi sit aequalis, neque ejus multiplo cuipiam, nulla quoque ejus potestas per P erit divisibilis, neque ergo in residuis cyphra unquam occurret.

4. Cum omnia residua sint divisore P minora, multitudo autem numerorum divisore P minorum sit $= P - 1$, plura residua diversa occurrere nequeunt quam $P - 1$. Quare cum series residuorum sit infinita, eadem residua in ea saepius recurrere debent.

5. Ex quolibet residuo, veluti ε, sequens ζ facile definitur. Cum enim sit $\varepsilon = a^5 - mP$ et $\zeta = a^6 - nP$, erit $\zeta - a\varepsilon = (ma - n)P$, hincque $\zeta = a\varepsilon - (n - ma)P$. Quare a producto $a\varepsilon$ auferatur divisor P quoties fieri potest, ac relinquetur residuum sequens ζ.

6. Respectu numeri primi P omnes numeri in certos ordines distribui possunt, ad eundem ordinem referendo omnes eos numeros, qui per P divisi idem relinquunt residuum, hi ergo ordines erunt:

I.	$0,$	$P,$	$2P,$	$3P,$	$4P \ldots\ldots\ldots mP,$
II.	$1,$	$P+1,$	$2P+1,$	$3P+1,$	$4P+1 \ldots\ldots mP+1,$
III.	$2,$	$P+2,$	$2P+2,$	$3P+2,$	$4P+2 \ldots\ldots mP+2,$
IV.	$3,$	$P+3,$	$2P+3,$	$3P+3,$	$4P+3 \ldots\ldots mP+3,$

etc.

7. Pro quolibet ergo numero primo P tot habentur numerorum ordines, quot unitates in numero P continentur: et quilibet ordo determinatur residuo, quod omnibus numeris ejus ordinis est commune, hocque residuum in quovis ordine locum occupat primum.

8. Cum cujusque ordinis natura residuo ipsi proprio determinetur, quilibet cujusque ordinis numerus ejus naturam perinde declarat, ac primus, qui ipsum residuum exhibet. Hinc nihil impedit, quominus idem residuum ε per quemlibet alium numerum ejusdem ordinis $mP + \varepsilon$ denotetur.

9. Ita idem residuum ε non solum per numeros positivos $\varepsilon + P$, $\varepsilon + 2P$ etc. indicare licebit, sed etiam per negativos $\varepsilon - P$, $\varepsilon - 2P$ etc. Cum igitur, si ε sit divisoris P semisse majus, $\varepsilon - P$ eodem sit minus, patet numeros negativos admittendo, omnia residua numeris, qui divisoris P semissem non superent, exprimi posse.

Observationes.

10. Proposito divisore primo P, prout progressionis geometricae radix a constituatur, fieri potest, ut in residuis vel omnes numeri ipso P minores occurrant, vel non omnes. Si enim sumatur radix $a = 1$, omnia residua in unitatem abeunt; ac si sumatur $a = P - 1$, series residuorum prodit:

$$1, \quad P-1, \quad 1, \quad P-1, \quad 1, \quad P-1 \quad \text{etc.}$$
$$\text{vel} \quad +1, \quad -1, \quad +1, \quad -1, \quad +1, \quad -1 \quad \text{etc.} \quad (9).$$

11. Quod autem interdum omnes numeri divisore P minores in residuis occurrunt, unico exemplo declarasse sufficiat; sit scilicet $P = 7$ et sumatur radix $a = 3$, habebitur:

progr. geom.	1,	3,	3^2,	3^3,	3^4,	3^5,	3^6,	3^7,	3^8,	3^9,	etc.
residua	1,	3,	2,	6,	4,	5,	1,	3,	2,	6,	etc.

12. Si pro eodem divisore $P = 7$ radici a alii valores tribuantur, series residuorum se habebunt ut sequitur:

progr. geom.	1,	2,	2^2,	2^3,	2^4,	2^5,	2^6,	2^7,	2^8,	2^9	etc.
residua	1,	2,	4,	1,	2,	4,	1,	2,	4,	1	etc.
progr. geom.	1,	4,	4^2,	4^3,	4^4,	4^5,	4^6,	4^7,	4^8,	4^9	etc.
residua	1,	4,	2,	1,	4,	2,	1,	4,	2,	1,	etc.
progr. geom.	1,	5,	5^2,	5^3,	5^4,	5^5,	5^6,	5^7,	5^8,	5^9	etc.
residua	1,	5,	4,	6,	2,	3,	1,	5,	4,	6	etc.

13. Ut omnes variationes, quae in serie residuorum locum habere possunt, obtineantur, sufficit radici a omnes valores divisore P minores tribuisse; si enim loco a sumatur $a + P$, ex progressione geometrica 1, $a + P$, $(a + P)^2$, $(a + P)^3$ etc. eadem residuorum series recurrit, quae ex grogressione geometrica 1, a, a^2, a^3, a^4, etc.

14. Quemadmodum in residuis etiam numeros negativos admittimus (9), ut ea infra semissem divisoris P deprimamus, ita etiam pro radice progressionis geometricae a numeros negativos assumere licet, ac tum habebitur:

progr. geom.	1,	$-a$,	$+a^2$,	$-a^3$,	$+a^4$,	$-a^5$,	$+a^6$,	$-a^7$	etc.
residua	1,	$-\alpha$,	β,	$-\gamma$,	δ,	$-\varepsilon$,	ζ,	$-\eta$	etc.

15. Sumta autem radice $-a$, eadem residua oriuntur, ac si radix poneretur $P - a$; unde patet, pro casibus, quibus radix a semissem divisoris P superat, residua ex casibus, quibus est $a < \frac{1}{2}P$, facile colligi.

16. Quodsi loco radicis a successive omnes numeri divisore P minores substituantur, series residuorum inde natae vel erunt completae vel incompletae: *completas* scilicet appello, in quibus omnes numeri divisore P minores occurrunt; *incompletas* vero, ubi quidam horum numerorum ex serie residuorum excluduntur.

17. Quoniam vidimus pro quovis divisore P dari ejusmodi valores radicis a, veluti si $a = 1$ et $a = P - 1$, ex quibus series residuorum incompletae resultant, hinc nascitur quaestio: *an semper ejusmodi progressiones geometricae exhiberi queant, unde series residuorum completae oriantur.*

18. Hujusmodi radices progressionis geometricae, quae series residuorum completas producunt, *primitivas* appellabo. Ita supra vidimus pro divisore $P = 7$ radices primitivas esse 3 et 5. Num autem pro omnibus divisoribus primis dentur radices primitivae, quaestio est altioris indaginis, infra decidenda.

Lemmata.

19. **Cum in serie residuorum termini praecedentes tandem recurrere debeant, primus qui recurrit semper est unitas.**

Demonstratio. Ponamus enim aliud quodvis residuum ε ex potestate a^μ natum recurrere, antequam unitas recurrat, idque secunda vice ex potestate $a^{\mu+\nu}$ prodire. Cum igitur sit $\varepsilon = a^\mu - mP$ et $\varepsilon = a^{\mu+\nu} - nP$, erit $a^{\mu+\nu} - a^\mu = (n - m) P$, ideoque $a^\mu (a^\nu - 1)$ multiplum ipsius P; at quia a^μ per numerum primum P dividi nequit, (radix enim a divisore P minor, ideoque ad eum prima statuitur), necessario alter factor $a^\nu - 1$ per P divisionem admittet, hincque potestas a^ν per P divisa unitatem relinquet; quae potestas cum inferior sit quam $a^{\mu+\nu}$ evidens est, residuum ε ante recurrere non posse, quam unitas recurrerit.

20. **Statim atque in serie residuorum 1, α, β, γ, δ etc. unitas iterum occurrit, deinceps eadem residua eodem ordine uti ab initio iterum recurrent.**

Demonstratio. Oriatur enim unitas secunda vice ex potestate a^ν, ac sequens residuum erit a, 1 (5) $= a$, idem quod ex secundo termino a nascebatur, ideoque α, post quod denuo sequentur residua β, γ, δ etc. eodem ordine uti ab initio.

21. **Si a sit radix primitiva, ejus potestas a^{P-1} per divisorem primum P divisa unitatem relinquet.**

Demonstratio. Quia a est radix primitiva, in serie residuorum omnes numeri divisore P minores occurrunt, quorum multitudo est $P - 1$; ex totidem ergo progressionis geometricae terminis $1, a^1, a^2, a^3$ etc. quorum ultimus erit a^{P-2}, oriantur necesse est; sequens ergo terminus a^{P-1} aliquod ex residuis praecedentibus reproducet, quod autem necessario est unitas (19).

22. **Si progressio geometrica 1, a, a^2, a^3, a^4 etc. seriem residuorum incompletam producat, numerus residuorum diversorum erit pars aliquota numeri $P - 1$, hoc est divisoris primi P unitate minuti.**

Demonstratio. Sit numerus residuorum diversorum 1, α, β, γ, δ etc. ex hac progressione geometrica natorum $= r$, qui ergo per hypothesin minor est quam $P - 1$, ita ut quidam numeri, qui sint $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc. eorumque multitudo $= P - 1 - r$, ex serie residuorum excludantur. Jam dico, quia $\mathfrak{A}$ in serie residuorum non reperitur, ibidem quoque nec $\alpha\mathfrak{A}$, nec $\beta\mathfrak{A}$, nec $\gamma\mathfrak{A}$ etc.

occurrere posse. Si enim $\varepsilon\mathfrak{A}$ esset residuum, quia ε ex certa potestate radicis a, quae sit a^ν, nascitur, loco $\varepsilon\mathfrak{A}$ spectare licet $a^\nu\mathfrak{A}$, unde sequentia residua forent $a^{\nu+1}\mathfrak{A}$, $a^{\nu+2}\mathfrak{A}$, $a^{\nu+3}\mathfrak{A}$ etc. et in genere $a^n\mathfrak{A}$; quia autem datur potestas a^n unitatem relinquens, hoc residuum foret $\mathfrak{A}$, contra hypothesin. Hinc dato uno non-residuo $\mathfrak{A}$, simul dantur r non-residua; quae si nondum multitudinem numerorum $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, etc. quorum numerus est $P-1-r$, exhauriant, de novo r non-residua accedunt, sicque porro; unde numerus $P-1-r$ necessario erit multiplus ipsius r; sit ergo $P-1-r=nr$, fiet $r=\frac{P-1}{n+1}$, ac propterea numerus residuorum r semper est pars aliquota numeri $P-1$.

23. Quicunque valor divisore primo P minor radici a tribuatur, potestas a^{P-1} per P divisa unitatem relinquit, seu formula $a^{P-1}-1$ per P erit divisibilis.

Demonstratio. Sit r numerus omnium residuorum diversorum 1, α, β, γ, δ etc. quae ergo nascuntur ex progressione geometrica

$$1,\ a,\ a^2,\ a^3,\ a^4 \ldots\ldots a^{r-1},$$

sequens igitur potestas a^r unitatem pro residuo habebit, eritque forma a^r-1 per divisorem P divisibilis. Quia vero r est pars aliquota numeri $P-1$, illa forma $a^{P-1}-1$ per hanc a^r-1 erit divisibilis, ideoque etiam per ipsum divisorem P.

24. In serie residuorum 1, α, β, γ, δ etc. sive fuerit completa, sive incompleta, simul producta ex binis, ternis, quaternis etc. hincque etiam singulorum potestates quaecunque, siquidem per divisorem P deprimantur, occurrunt.

Demonstratio. Si enim potestas a^m residuum relinquat μ, et potestas a^n residuum ν, erit $a^m = ..P+\mu$ et $a^n = ..P+\nu$, ubi duo puncta .. loco cujusvis indicis integri scribo, hincque $a^{m+n} = ..P+\mu\nu$, ita ut potestas a^{m+n} residuum $\mu\nu$ sit relictura. Quare cum productum binorum quorumcunque residuorum in serie residuorum occurrat, propositum est manifestum.

25. Datis duobus residuis μ et ν, in serie residuorum etiam aliquod reperietur ω, ut sit $\nu=\mu\omega$, vel $\nu=\mu\omega-..P$.

Demonstratio. Oriantur enim residua μ et ν a potestatibus a^m et a^n, ac sit ω residuum a potestate a^{n-m}, vel hac $a^{P-1+n-m}$, si forte fuerit $n<m$, eritque potestatis $a^n=a^m.a^{n-m}$ residuum $=\mu\omega-..P$, ideoque $\nu=\mu\omega-..P$.

26. Cum unitas semper in serie residuorum contineatur, cuique residuo μ respondebit ibidem aliud quoddam ω, ut sit $\mu\omega=1$, seu $\mu\omega=1+..P$. Hujusmodi bina residua *socia* appellabo. Unde patet, in omni serie residuorum terminos ita sociatim exhiberi posse, ut bina quaeque sibi sint socia. Hoc tantum notetur, unitatem sibi ipsi esse sociam, ac si -1 occurrat, socium quoque ipsi esse aequalem.

27. His praemissis, quae alibi fusius pertractavi, ad sequentia theoremata progredior, in quibus plures novae veritates ex principiis prorsus singularibus demonstrabuntur, ad quas per methodos adhuc usurpatas accessus nimis difficilis videtur.

28. **Theorema.** Ut forma x^n-1 per numerum primum P divisibilis evadat, sumendo $x<P$, id pluribus quam n modis fieri nequit.

Demonstratio. A casibus simplicissimis inchoemus, ac primo statim manifestum est formam $x^1 - 1$ per numerum primum P unico modo divisibilem esse posse sumendo $x = 1$, cum valores ipsius x divisore P majores excludantur.

Ut forma $x^2 - 1$ divisionem per numerum primum P admittat, vel $x - 1$, vel $x + 1$ divisionem admittere debet; priori casu fit $x = 1$, posteriori $x = P - 1$: neque ullo alio modo id evenire potest, siquidem casus $x > P$ excluduntur. Forma $x^3 - 1 = (x - 1)(xx + x + 1)$ per P divisibilis est primo si $x = 1$, tum vero si $xx + x + 1 = mP$, quod si eveniat casu $x = a$, etiam casu $x = a^2$ succedet; altiores enim potestates, ob $a^3 - 1$ divisibile per P, ideoque residuum ipsius $a^3 = 1$, ad praecedentes reducuntur. Jam vero dico praeter hos tres casus alios dari nullos; si enim divisio succederet quoque casu $x = b$, ob $aa + a + 1$ et $bb + b + 1$ per P divisibiles, differentia $(a - b)(a + b + 1)$ etiam esset divisibilis, hoc est vel $a - b$, vel $a + b + 1$; prius daret $b = a$, posterius ab $aa + a + 1$ ablatum praeberet $aa - b = mP$, hoc est $b = aa$, qui sunt casus jam enumerati. Unde pluribus quam tribus modis divisio non succedit.

Jam pro forma $x^n - 1$ in genere observo, si ea per numerum primum P fuerit divisibilis casu $x = a$, ut sit $x - a$ divisor formae $x^n - 1 - mP$, tum facta divisione oriri formam uno gradu inferiorem, per P divisibilem reddendam; quod si praestet valor $x = b$, denuo ad formam inferiorem pervenietur, ex quo perinde atque in resolutione aequationum concluditur, pluribus quam n modis quaesitum obtineri non posse; qui si $x = a$ fuerit unus valor idoneus, erunt

$$x = 1, \quad x = a, \quad x = a^2, \quad x = a^3, \quad x = a^4, \ldots . x = a^{n-1}$$

quandoquidem a^n iterum unitati aequivalet.

29. **Scholion.** Theorema hoc ita accipi debet, ut forma $x^n - 1$ certe non pluribus quam n modis per numerum primum P divisibilis reddi queat, aliis pro x valoribus non admittendis, nisi qui ipso P sint minores. Cum enim si quispiam valor $x = a$ id praestet, omnes in hac formula $x = a + mP$ idem sint praestaturi, hos omnes pro unico casu haberi convenit. Hac lege constituta saepius evenire potest, ut numerus casuum sit minor quam exponens n; veluti si quaestio sit, quot casibus forma $x^5 - 1$ per 7 divisibilis existat, hoc non quinque, sed unico modo $x = 1$ fieri posse deprehenditur, dum reliqui quatuor casus quasi fiunt imaginarii. Ex sequentibus autem patebit, semper quasdam solutiones fieri impossibiles, quoties exponens n non fuerit pars aliquota ipsius $P - 1$, dum contra, quoties n est pars aliquota ipsius $P - 1$, omnes solutiones sunt reales. Ac si $n = P - 1$, tum manifesto totidem habentur solutiones, quia omnes numeri ipso P minores, quorum multitudo est $P - 1$, loco x positi formulam $x^n - 1$ per numerum primum P divisibilem reddunt (22). Quando autem exponens n major est quam $P - 1$, veluti $n = P - 1 + k$, tum forma $x^{P-1+k} - 1$ reducitur ad $x^k - 1$, quoniam potestas x^{P-1} ratione residuorum unitati aequivalere est censenda.

30. **Definitio.** Casus *proprii*, quibus formula $x^n - 1$ per quempiam numerum primum divisibilis esse potest, sunt ii, qui ipsi cum nulla forma inferiori, ubi exponens n est minor, sunt communes.

31. **Coroll. 1.** Quia casus $x = 1$ formulae $x^n - 1$ cum omnibus inferioribus est communis, hunc semper a casibus formulae isti propriis excludi oportet: unde cum numerus omnium casuum sit n, numerus casuum propriorum saltem unitate est minor.

32. **Coroll. 2.** Si exponens n fuerit numerus primus, formula $x^n - 1$ per nullam inferiorem ejusdem formae divisibilis est praeter $x^1 - 1$, unde numerus casuum propriorum est $n - 1$.

33. **Coroll. 3.** Sin autem exponens n fuerit numerus compositus, puta $n = \mu\nu$, tum formula $x^n - 1$ iisdem casibus est divisibilis, quibus formulae $x^\mu - 1$ et $x^\nu - 1$, quandoquidem ipsa per has divisibilis existit; unde casus harum formularum a casibus propriis formulae $x^n - 1$ sunt segregandi.

34. **Problema.** Pro omnibus exponentibus n numerum casuum propriorum definire, quibus formula $x^n - 1$ per quempiam numerum primum P divisibilis reddi potest, alios pro x valores non admittendo, nisi qui divisore sint minores.

Solutio. A numero omnium casuum, qui est $= n$, excludantur casus, quibus formulae inferiores in proposita contentae simul fiunt divisibiles; aliae autem formulae inferiores veluti $x^\nu - 1$ in proposita $x^n - 1$ non continentur, nisi quarum exponens ν est pars aliquota exponentis n. Verum si plures hujusmodi formulae inferiores dentur, ne iidem casus bis vel pluries excludantur, tantum casus cuique proprii excludi debent, quo facto remanebunt casus formulae propositae $x^n - 1$ proprii; hoc modo ab exponentibus minoribus ad continuo majores facile progredi licet:

formula	numerus casuum propriorum
$x^1 - 1$	1
$x^2 - 1$	$2 - 1 = 1$
$x^3 - 1$	$3 - 1 = 2$
$x^4 - 1$	$4 - 1 - 1 = 2$
$x^5 - 1$	$5 - 1 = 4$
$x^6 - 1$	$6 - 2 - 1 - 1 = 2$
$x^7 - 1$	$7 - 1 = 6$
$x^8 - 1$	$8 - 2 - 1 - 1 = 4$
$x^9 - 1$	$9 - 2 - 1 = 6$

etc.

Hinc in genere si α, β, γ, δ etc. sint numeri primi, res ita se habebit:

formula	numerus casuum propriorum
$x^1 - 1$	1
$x^\alpha - 1$	$\alpha - 1$
$x^\beta - 1$	$\beta - 1$
$x^\gamma - 1$	$\gamma - 1$
$x^{\alpha\alpha} - 1$	$\alpha\alpha - \alpha = \alpha(\alpha - 1)$
$x^{\alpha\beta} - 1$	$\alpha\beta - \alpha - \beta + 1 = (\alpha - 1)(\beta - 1)$
$x^{\beta\beta} - 1$	$\beta\beta - \beta = \beta(\beta - 1)$
$x^{\alpha\gamma} - 1$	$\alpha\gamma - \alpha - \gamma + 1 = (\alpha - 1)(\gamma - 1)$
$x^{\beta\gamma} - 1$	$\beta\gamma - \beta - \gamma + 1 = (\beta - 1)(\gamma - 1)$
$x^{\gamma\gamma} - 1$	$\gamma\gamma - \gamma = \gamma(\gamma - 1)$
$x^{\alpha\alpha\alpha} - 1$	$\alpha^3 - \alpha\alpha + \alpha - \alpha + 1 - 1 = \alpha\alpha(\alpha - 1)$
$x^{\alpha\alpha\beta} - 1$	$\alpha\alpha\beta - \alpha\alpha + \alpha - (\alpha - 1)(\beta - 1) - \alpha - \beta + 1 = \alpha(\alpha - 1)(\beta - 1)$

unde colligimus, si fuerit $n = \alpha^\lambda \beta^\mu \gamma^\nu$, pro formula $x^n - 1$ fore numerum casuum propriorum

$$\alpha^{\lambda-1}(\alpha-1)\beta^{\mu-1}(\beta-1)\gamma^{\nu-1}(\gamma-1).$$

Quae si attentius contemplemur, mox deprehendemus pro qualibet formula $x^n - 1$ tot dari casus proprios, quot infra exponentem n dantur numeri ad ipsum primi.

35. **Coroll. 1.** Divisore primo existente $= P$, si exponens n sumatur $= P - 1$, quia formula $x^{P-1} - 1$ certo habet $P - 1$ casus eosque omnes reales, cum x omnes valores ipso P minores recipere queat; si inde expungantur ii, qui huic formulae cum simplicioribus sunt communes, casus proprii, qui relinquuntur, omnes certo erunt reales.

36. **Coroll. 2.** Hinc semper ejusmodi dantur numeri divisore P minores, qui casus formulae $x^{P-1} - 1$ proprios exhibent, ita ut iidem casus nulli formulae inferiori conveniant.

37. **Scholion.** Quamvis haec nimis abstracta et omni usu destituta videantur, tamen equidem iis supersedere non potui in sequentibus demonstrationibus adornandis, ubi imprimis ante omnia est ostendendum, quicunque numerus primus pro divisore P accipiatur, semper ejusmodi progressiones geometricas $1, a, a^2, a^3, a^4$ etc. exhiberi posse, unde series residuorum completae resultent, in quibus scilicet omnes numeri divisore P minores occurrant, antequam idem residuorum ordo revertatur. Plerisque forte haec res ita manifesta videbitur, ut demonstratione non egeat, cum pro minoribus divisoribus primis hujusmodi progressiones geometricae series residuorum completas praebentes, actu exhiberi queant, pro majoribus autem ratio dubitandi continuo decrescere videatur. Verum quoniam hoc secus evenit pro divisoribus non-primis, haec numerorum primorum proprietas utique demonstrationem postulare est visa.

38. **Theorema.** Quicunque numerus primus pro divisore P accipiatur, semper ejusmodi progressio geometrica $1, a, a^2, a^3, a^4$ etc. exhiberi potest, ex qua series residuorum completa oriatur.

Demonstratio. Cum posita in genere progressionis geometricae radice x, minore semper quam divisor P, terminus x^{P-1} per P divisus unitatem relinquat, indeque residua eodem ordine uti ab initio revertantur; ostendi oportet pro x ejusmodi numerum a assumi posse, ut a^{P-1} sit ejus infima potestas, quae per P divisa unitatem relinquat; quia enim tum in serie residuorum unitas ante hunc terminum non occurrit omnia antecedentia residua inter se diversa sint necesse est, quorum numerus cum sit $= P - 1$, omnes numeri divisore P minores in serie residuorum reperientur, eaque propterea erit completa. Res itaque huc redit, ut ostendatur, non omnes numeros divisore P minores ita esse comparatos, ut eorum inferior quaepiam potestas per P divisa unitatem relinquat. Verum si hoc eveniat in potestate x^n existente $n < P - 1$, jam ostendimus (§ 21), ejus exponentem n esse necessario partem aliquotam ipsius $P - 1$; cum jam § 34 docuerim, formam $x^{P-1} - 1$ semper habere casus sibi proprios, puta $x = a$, ut nulla inferior divisionem per P admittat: perspicuum est potestatem a^{P-1} fore infimam, quae per P divisa unitatem relinquat; unde sumto tali numero a pro radice progressionis geometricae, ex ea series residuorum completa oriatur necesse est.

39. **Scholion.** Quo haec clarius intelligantur, conveniet pro simplicioribus divisoribus primis tales series residuorum completas conspectui exponi, ubi quidem progressiones geometricas, unde nascuntur, non opus est exponi, quia radix semper secundo termino seriei residuorum est aequalis;

sed sufficiet generalem progressionem in capite posuisse, ut inde exponentes, quibus singuli termini in seriebus residuorum respondent, perspiciantur:

Divisor primus	a^0	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}	a^{19}	a^{20}	etc.
3	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2 etc.
5	1	2	4	3	1	2	4	3	1	2	4	3	1	2	4	3	1	2	4	3	1	2 etc.
7	1	3	2	6	4	5	1	3	2	6	4	5	1	3	2	6	4	5	1	3	2	6 etc.
11	1	2	4	8	5	10	9	7	3	6	1	2	4	8	5	10	9	7	3	6	1	2 etc.
13	1	2	4	8	3	6	12	11	9	5	10	7	1	2	4	8	3	6	12	11	9	5 etc.
17	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	3	9	10	13	5 etc.
19	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1	2	4	8 etc.
23	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14 etc.

Radices igitur, quibus hic pro istis divisoribus primis sumus usi, sunt primitivae, quia earum potestates omnia diversa residua divisore minora suppeditant, quibus exhaustis demum unitas recurrit, et series eodem ordine uti ab initio progrediuntur. Via quidem adhuc non patet, tales radices primitivas pro quovis divisore primo inveniendi, neque etiam demonstratio, qua tales radices primitivas semper dari evici, methodum eas inveniendi declarat. Pro quovis autem divisore primo radix hujusmodi primitiva tentando non difficulter elicitur. Veluti pro divisore 23, primum radicem $a = 2$ assumo, unde haec series residuorum nascitur:

$$1,\ 2,\ 4,\ 8,\ 16,\ 9,\ 18,\ 13,\ 3,\ 6,\ 12,\ 1,$$

quae cum sit incompleta, jam inde patet radicem primitivam inter numeros exclusos quaeri debere, quorum minimus 5 negotium conficere deprehenditur; nisi hoc accidisset, denuo inter numeros exclusos radicem primitivam quaesivissem.

40. **Theorema.** Si divisor primus sit $P = 2n + 1$, et a radix primitiva, tum progressionis geometricae 1, a, a^2, a^3 etc. terminus a^n residuum praebet $2n$ seu -1.

Demonstratio. Cum a sit radix primitiva, ejus potestas a^{2n} per divisorem $2n + 1$ divisa unitatem relinquit, neque ulla datur potestas inferior idem praestans; formula ergo $a^{2n} - 1$ per eundem divisorem erit divisibilis, neque ulla alia inferior. Cum igitur sit $a^{2n} - 1 = (a^n - 1)(a^n + 1)$, et factor $a^n - 1$ non sit per divisorem $2n + 1$ divisibilis, alterum factorem $a^n + 1$ divisibilem esse necesse est, seu erit $a^n + 1 = m(2n + 1)$ hincque

$$a^n = m(2n + 1) - 1, \text{ vel } a^n = (m - 1)(2n + 1) + 2n;$$

unde manifestum est potestatem a^n per divisorem $2n + 1$ divisam relinquere -1 seu $2n$.

41. **Coroll. 1.** Si ergo residua ex initio progressionis geometricae 1, a, a^2, a^3, etc. nata sint 1, α, β, γ etc. residua ex terminis a^n, a^{n+1}, a^{n+2}, a^{n+3} etc. nata erunt -1, $-\alpha$, $-\beta$, $-\gamma$ etc., seu $2n$, $2n + 1 - \alpha$, $2n + 1 - \beta$, $2n + 1 - \gamma$ etc. cum sit $\alpha = a$, $\beta = a\alpha$, $\gamma = a\beta$ etc. semperque sequens terminus oriatur ex praecedente per radicem a multiplicato.

42. **Coroll. 2.** Series ergo residuorum completa, cujus terminorum numerus est $= 2n$, antequam iidem termini recurrant, in duas partes dispescitur 1, α, β, γ, δ etc. et -1, $-\alpha$,

$-\beta$, $-\gamma$, etc. cujus posterioris termini sunt complementa terminorum prioris; seu residua ex terminis a^λ et $a^{n+\lambda}$ nata simul sumta sunt $=0$, sive divisorem $2n+1$ praebent.

43. **Scholion.** Quae de binis residuis sociis supra sunt observata, quorum productum unitate superat multiplum divisoris, ea hic ita sunt disposita, ut a medio, quod est -1 vel $2n$ aequidistent. Si enim r et s sint residua ex potestatibus $a^{n+\nu}$ et $a^{n-\nu}$ nata, productum rs erit residuum ex potestate a^{2n} natum, quod cum sit unitas, erit $rs=1$, vel $1+m(2n+1)$. Ipsum autem residuum medium -1, seu $2n$, sibi ipsum est socium, omnino uti primum $+1$ se ipsum habet pro socio. Reliqua residua sociata omnia sunt inaequalia, et quocunque proposito r, alterum sibi socium s erit $=\frac{1+m(2n+1)}{r}$; semper enim m ita definire licet, ut $m(2n+1)+1$ per r divisionem admittat, siquidem, uti assumsimus $2n+1$ fuerit numerus primus, et r numerus ipso minor, vel saltem ad eum primus. Quemadmodum autem in nostra serie residua sunt disposita, cujusque socium expedite reperitur, cum ambo a medio -1 aequidistent.

44. **Theorema.** Si divisor fuerit numerus quicunque primus P, tot dantur radices primitivae, quot reperiuntur numeri ad $P-1$ primi eoque minores, quandoquidem tantum radices divisore minores consideramus.

Demonstratio. Ponamus $P-1=Q$, et cum certe detur radix primitiva, sit ea $=a$, ita ut a^Q sit minima potestas ipsius a per P divisa unitatem relinquens. Tum vero sit n numerus quicunque primus ad Q, ac potestas a^n per divisorem P divisa relinquat residuum b, quod utique ab a erit diversum; eritque b itidem radix primitiva, seu quod eodem redit, ipsa potestas a^n uti radix primitiva spectari potest. Ad quod demonstrandum ostendi debet in progressione geometrica

$$1,\ a^n,\ a^{2n},\ a^{3n},\ \ldots\ldots\ a^{Qn}$$

ante terminum a^{Qn} nullum occurrere, qui per P divisus unitatem relinquat. Jam quia a est radix primitiva, nullae aliae ejus potestates per P divisae unitatem relinquunt, nisi quarum exponentes sint vel Q, vel $2Q$, vel $3Q$, vel multiplum quodcunque ipsius Q, unde quidem manifestum est potestatem a^{Qn} unitatem relinquere. Simul vero patet, quia numerus n ad Q est primus, nullum multiplum ipsius n minus quam Qn simul esse multiplum ipsius Q; si enim mn existente $m<Q$ esset multiplum ipsius Q, puta $=kQ$, ob $mn=kQ$ foret $m:Q=k:n$, ideoque numeri n et Q non forent inter se primi. Quare cum in superiori progressione geometrica ante terminum a^{Qn} nullus alius occurrat, qui per divisorem P divisus unitatem relinquat, series residuorum inde nata Q terminos diversos complectetur, eritque propterea completa, et a^n seu residuum inde natum b erit radix primitiva. Cum igitur ex quolibet numero n ad Q seu $P-1$ primo obtineatur radix primitiva, admissa una saltem primitiva a, manifestum est, semper tot dari radices primitivas, quot dantur numeri ad numerum $Q=P-1$ primi, eoque minores, quandoquidem radices majores ab hac consideratione excludimus.

45. **Coroll. 1.** Pro divisore ergo $P=3$ et $Q=2$, unica datur radix primitiva 2 ex potestate a^1 nata; pro divisore $P=5$ et $Q=4$ duae dantur 2 et 3 ex potestatibus a^1 et a^3 natae. Pro divisore $P=7$ et $Q=6$, iterum duae dantur 3 et 5 ex potestatibus a^1 et a^5 natae. Pro divisore $P=11$ et $Q=10$, ad quem numerum Q primi sunt 1, 3, 7, 9, radices primitivae sunt

2, 8, 7, 6, ex potestatibus a^1, a^3, a^7, a^9 natae, uti ex seriebus residuorum completis § 38 allatis perspicitur.

46. **Coroll. 2.** Pro quovis ergo divisore primo P multitudo radicum primitivarum multitudini numerorum ad numerum $Q = P - 1$ primorum eoque minorum est aequalis, ideoque ex compositione numeri Q est indicanda. Ita si fuerit $Q = \alpha^\lambda \beta^\mu \gamma^\nu$ etc. existentibus α, β, γ etc. numeris primis, constat numerum radicum primitivarum fore

$$= \alpha^{\lambda - 1}(\alpha - 1) \,.\, \beta^{\mu - 1}(\beta - 1) \,.\, \gamma^{\nu - 1}(\gamma - 1) \text{ etc.}$$

47. **Coroll. 3.** Ipsi autem numeri ad Q primi facile reperiuntur, dum ex numeris omnibus ipso Q minoribus expunguntur ii, qui ad Q sunt compositi: qui enim restant, inter quos semper unitas reperitur, erunt ad Q primi.

48. **Scholion.** Ex data theorematis demonstratione autem simul intelligitur, plures non dari radices primitivas, quam assignavimus. Sumta enim quacunque alia potestate radicis primitivae jam cognitae a, puta a^m, cujus exponens m non sit primus ad Q, sed cum Q communem habeat divisorem, qui sit d, ut tam $\frac{Q}{d}$ quam $\frac{m}{d}$ sit numerus integer; in progressione geometrica 1, a^m, a^{2m}, a^{3m}, a^{4m} etc. occurret potestas, cujus scilicet exponens $= \frac{Q}{d} m$, antequam ad a^{Qm} perveniatur, qui cum sit quoque $= \frac{m}{d} Q$, ideoque multiplum ipsius Q, ex ea potestate jam orietur residuum 1, ac propterea series residuorum prodibit incompleta. Talis ergo potestas a^m seu residuum inde resultans certe non erit radix primitiva.

49. **Coroll. 4.** Si residuum r praebeat radicem primitivam, etiam ejus socium s dabit radicem primitivam. Posito enim divisore primo $P = 2n + 1$, ut sit $Q = 2n$, sit $a^{n-\lambda}$ potestas praebens residuum r, et socium s resultat ex potestate $a^{n+\lambda}$. Evidens autem est si $n - \lambda$ fuerit ad $Q = 2n$ primus, tum etiam exponentem alterum $n + \lambda$ fore ad Q primum.

50. **Scholion.** Haud abs re fore arbitror, si pro simplicioribus divisoribus primis P tam numeros ad $Q = P - 1$ primos, quam radices primitivas iis respondentes conspectui exposuero:

Divisor primus	
3	1 ad 2 primus
	2 radix primitiva
5	1, 3 primi ad 4
	2, 3 radices primitivae
7	1, 5 primi ad 6
	3, 5 radices primitivae
11	1, 3, 7, 9 primi ad 10
	2, 8, 7, 6 radices primitivae
13	1, 5, 7, 11 primi ad 12
	2, 6, 11, 7 radices primitivae

Divisor primus	
17	1, 3, 5, 7, 9, 11, 13, 15 primi ad 16
	3, 10, 5, 11, 14, 7, 12, 6 radices primitivae
19	1, 5, 7, 11, 13, 17 primi ad 18
	2, 13, 14, 15, 3, 10 radices primitivae
23	1, 3, 5, 7, 9, 13, 15, 17, 19, 21 primi ad 22
	5, 10, 20, 17, 11, 21, 13, 15, 7, 14 radices primitivae
29	1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27 primi ad 28
	2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11, 15 radices primitivae
31	1, 7, 11, 13, 17, 19, 23, 29 primi ad 30
	3, 17, 13, 24, 22, 12, 11, 21 radices primitivae
37	1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35 primi ad 36
	2, 32, 17, 13, 15, 18, 35, 5, 20, 24, 22, 19 radices primitivae.

Nullam autem hic inter quemque numerum primum et radices primitivas ipsi convenientes relationem deprehendere licet, ex qua pro quovis divisore primo saltem unica radix primitiva colligi posset; atque adeo ordo inter istas radices aeque absconditus videtur, ac inter ipsos numeros primos.

51. **Theorema.** Si numeri quadrati per quempiam divisorem primum P dividantur, residua inde orta, nisi sint 0, in serie residuorum completa potestatibus parium exponentium respondent.

Demonstratio. Sit pro divisore primo P radix quaedam primitiva a, ut haec progressio geometrica

$$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7 \text{ etc.}$$

seriem residuorum completam praebeat, in qua omnes numeri divisore minores occurrant. Si jam xx quadratum quodcunque per P dividendum, et r residuum ex divisione radicis x ortum, ut sit $x = mP + r$; ac si $r = 0$, seu x multiplum divisoris P, etiam residuum ex quadrato xx natum erit $= 0$, quos casus, cum per se sint perspicui, hic non consideramus. At si r sit numerus quicunque divisore P minor, quia in serie residuorum completa certe continetur, ex certa quadam potestate ipsius a, quae sit a^λ nascatur necesse est, tum autem residuum ex divisione quadrati xx oriundum conveniet cum eo, quod ex divisione potestatis $a^{2\lambda}$ nascitur; sicque ex divisione quadratorum alia residua resultare nequeunt, nisi quae ex potestatibus formae $a^{2\lambda}$, hoc est, quarum exponentes sunt numeri pares, oriuntur.

52. **Coroll. 1.** Residua ergo, quae ex divisione quadratorum per divisorem primum P nascuntur, convenient cum iis residuis, quae ex hac progressione geometrica nascuntur

$$1,\ a^2,\ a^4,\ a^6,\ a^8,\ a^{10},\ a^{12} \text{ etc.}$$

existente a radice primitiva.

53. **Coroll. 2.** Si ergo divisor primus sit $P=2n+1$, quam formam omnes numeri primi praeter binarium habent, quia 2 non est numerus primus ad $P-1=2n$, etiam a^2 non erit radix primitiva, ideoque series residuorum ex quadratis oriunda non erit completa.

54. **Coroll. 3.** Quia autem a^{2n} est minima potestas radicis a unitatem relinquens, multitudo residuorum, quae ex numeris quadratis resultare possunt, certo est $=n$, cyphra exclusa; totidemque numeri nunquam possunt esse residua quadratorum, quos proinde non-residua appellavi.

55. **Scholion 1.** Hoc etiam ex serie residuorum completa facillime perspicitur, quae si progressioni geometricae subscripta fuerint

$$1,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ a^7 \ldots\ldots a^{2n}$$
$$1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \varepsilon,\ \zeta,\ \eta \ldots\ldots 1$$

ex divisione quadratorum nascitur haec series residuorum

$$1,\ \beta,\ \delta,\ \zeta \ldots\ldots 1,$$

quorum multitudo manifesto est semissis illorum, quoniam serie etiam continuata eadem eodem ordine recurrunt.

Hinc uti residua quadratorum sunt $1,\ \beta,\ \delta,\ \zeta$ etc. ita non-residua erunt $\alpha,\ \gamma,\ \varepsilon,\ \eta$ etc. numero totidem, nisi scilicet binarius pro divisore primo accipiatur. Quare cum ex serie quadratorum 1, 4, 9, 16 usque ad $4nn$ continuata omnia residua diversa oriri debeant, horumque quadratorum numerus sit $2n$, residuorum vero numerus tantum $=n$, necesse est ex binis horum quadratorum aequalia residua nasci, quod adeo per se est perspicuum, cum quadrata bb et $(2n+1-b)^2$ per divisorem $2n+1$ divisa idem residuum relinquant.

56. **Scholion 2.** Simili modo ostendi potest, residua, quae ex divisione cuborum nascuntur, non discrepare ab iis, quae progressioni geometricae $1,\ a^3,\ a^6,\ a^9,\ a^{12}$ etc. conveniunt, denotante a semper radicem primitivam: Atque in genere si potestates numerorum quaecunque:

$$1,\ 2^\lambda,\ 3^\lambda,\ 4^\lambda,\ 5^\lambda,\ 6^\lambda,\ 7^\lambda \text{ etc.}$$

per numerum primum P dividantur, residua inde oriunda eadem erunt atque ea, quae ex hac progressione geometrica nascuntur:

$$1,\ a^\lambda,\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda},\ a^{5\lambda},\ a^{6\lambda} \text{ etc.}$$

existente a radice primitiva pro divisore primo P; unde patet, si exponens λ fuerit numerus ad $P-1$ primus, seriem residuorum fore completam; at si exponens λ ad $P-1$ non sit primus, ac maximus eorum communis divisor fuerit $=d$, tum utique in residuis non omnes numeri occurrent, sed tot tantum, ut eorum multitudo sit $=\frac{P-1}{d}$, cujus ratio ex hactenus allatis satis est manifesta. Sed antequam altiores potestates accuratius scrutemur, quasdam insignes proprietates circa residua quadratorum explicasse juvabit.

57. **Theorema.** Divisore primo posito $P=2n+1$, in residuis quadratorum occurret numerus -1 seu $2n$ quoties n fuerit numerus par; sin autem n sit numerus impar, tum -1 seu $2n$ certe non reperietur in residuis, sed erit non-residuum.

Demonstratio. Cum progressio geometrica $1,\ a^2,\ a^4,\ a^6,\ a^8$ etc. omnia producat residua quadratorum, evidens est in ea occurrere terminum a^n si quidem n sit numerus par; at supra vidi-

mus potestatem a^n semper dare residuum -1 seu $2n$; ex quo manifestum est, quoties n fuerit numerus par, toties in residuis quadratorum reperiri -1 seu $2n$, contra vero si n fuerit impar, $2n$ seu -1 erit non-residuum.

58. **Coroll. 1.** Pro omnibus ergo divisoribus primis formae $4n+1$ in residuis quadratorum certe occurrit -1 seu $4n$, et cum productum ex binis residuis iterum sit residuum, si residuum quodcunque fuerit α, etiam $-\alpha$ in residuis reperietur: scilicet cujusque residui complementum quoque est residuum.

59. **Coroll. 2.** Pro divisoribus autem primis formae $4n-1$, in residuis quadratorum certe non occurrit -1, sed erit non-residuum; hinc cum productum ex residuo et non-residuo semper sit non-residuum, omnium residuorum complementa erunt non-residua.

60. **Theorema.** Proposito numero primo formae $4n+1$, semper summa duorum quadratorum ad eum primorum exhiberi potest, quae sit per eum divisibilis, atque alterum quidem quadratum pro lubitu accipere licet.

Demonstratio. Sumto enim quadrato quocunque bb, quod per $4n+1$ divisum relinquat residuum β, dabitur semper aliud quadratum xx quod per $4n+1$ divisum relinquet residuum $-\beta$ seu $4n+1-\beta$, ex quo summa horum duorum quadratorum $bb+xx$ per numerum primum $4n+1$ divisibilis sit necesse est; et cum neutrum per se divisionem admittat, ea utique ad $4n+1$ erunt prima.

61. **Coroll. 1.** Evidens quoque est quadratum xx infinitis modis accipi posse, cum omnia quadrata in hac forma $(m(4n+1)\pm x)^2$ idem residuum, quod xx praebeant: unde pro x dabitur valor non solum minor quam $4n+1$, sed etiam minor ejus semisse $\frac{4n+1}{2}$ seu minor quam $2n+1$.

62. **Coroll. 2.** Semper ergo tales summae binorum quadratorum:

$$1+pp, \quad 4+qq, \quad 9+rr, \quad 16+ss, \quad 25+tt \text{ etc.}$$

exhiberi possunt, quae omnes sint per numerum primum $4n+1$ divisibiles; atque ita ut singulorum radices sint minores quam $2n+1$.

63. **Coroll. 3.** Cum multitudo numerorum minorum quam $2n+1$ sit $=2n$, ac semper bina quadrata disparia jungantur, multitudo harum formularum erit n: et quia talis summa binorum quadratorum minor est quam $2(2n+1)^2 = 8nn+8n+2$, quotus erit minor quam $2n+\frac{1}{2}$ seu $2n+2$.

64. **Scholion.** Quo has summas binorum quadratorum pro quovis numero primo formae $4n+1$ facilius elicere queamus, residua ex quadratis orta pro simplicioribus apponamus:

Num. primi formae $4n+1$	Quadrata																		
	1,	4,	9,	16,	25,	36,	49,	64,	81,	100,	121,	144,	169,	196,	225,	256	etc.		
	Residua																		
5	1,	−1,	−1,	1,	0														
13	1,	4,	−4,	3,	−1,	−3.	−3,	−1,	3,	−4,	4,	1,	0						
17	1,	4,	−8,	−1,	8,	2,	−2,	−4,	−4,	−2,	2,	8,	−1,	−8,	4,	1			
29	1,	4,	9,	−13,	−4,	7,	−9,	6,	−6,	13,	5,	−1,	−5,	−7,	−7,	−5			
37	1,	4,	9,	16,	−12,	−1,	12,	−10,	7,	−11,	10,	−4,	−16,	11,	3,	−3,	−7,	−9,	−9.

Hinc pro his divisoribus formae $4n + 1$ sequentes habebimus binorum quadratorum summas per eos divisibiles:

Divisor 5	1								
	4								
summa	5								
quotus	1.								

Divisor 13	1	4	16						
	25	9	36						
summae	26	13	52						
quoti	2	1	4.						

Divisor 17	1	4	9	36					
	16	64	25	49					
summae	17	68	34	85					
quoti	1	4	2	5.					

Divisor 29	1	4	9	16	36	64	121		
	144	25	49	100	196	81	169		
summae	145	29	58	116	232	145	290		
quoti	5	1	2	4	8	5	10.		

Divisor 37	1	4	9	16	25	64	81	100	225
	36	144	324	169	49	121	289	196	256
summae	37	148	333	185	74	185	370	296	481
quoti	2	4	9	5	2	5	10	8	13.

Si igitur demonstrari posset in his quotis semper unitatem reperiri, haberetur demonstratio completa theorematis Fermatiani, quod omnis numerus primus formae $4n + 1$ sit summa duorum quadratorum. Quoniam vero alibi demonstravi summam duorum quadratorum inter se primorum alios divisores non admittere, nisi qui ipsi sint summae duorum quadratorum, demonstratio jam pro absoluta est habenda, quae multo concinnior est ea, quam olim per plures ambages elicueram. Sin autem simul perpendamus, in quotis illis nullos numeros primos formae $4n - 1$ occurrere posse, uti mox demonstrabitur, haec demonstratio forte multo magis contrahi poterit.

65. **Theorema.** Nulla summa duorum quadratorum inter se primorum per ullum numerum primum formae $4n - 1$ divisibilis existit.

Demonstratio. Quia sumto quocunque quadrato bb, quod per $4n - 1$ divisum praebeat residuum β, numerus $-\beta$ seu $4n - 1 - \beta$ ex residuis quadratorum prorsus excluditur (58), nullumque datur quadratum, quod ipsi bb additum summam producat per numerum primum $4n - 1$ divisibilem.

66. **Coroll. 1.** Summa ergo duorum quadratorum nullum divisorem admittit formae $4n - 1$, etiamsi hic divisor non sit primus; quoniam tum inter ejus factores semper unus saltem primus formae $4n - 1$ contineretur, nisi forte ambo quadrata seorsim per eum fuerint divisibilia.

67. **Coroll. 2.** Quando ergo summa duorum quadratorum per numerum primum formae $4n+1$ est divisibilis, quotus inde resultans neque erit formae $4n-1$, neque ullum habebit factorem primum hujus formae, nisi forte ambo quadrata hujusmodi habuerint communem divisorem, quo casu quotus adeo quadratum talis numeri contineret.

68. **Coroll. 3.** Ex ordine quotorum ergo, qui supra ex divisione summae binorum quadratorum per numerum primum formae $4n+1$ sunt orti, excluduntur hi numeri:

$$3,\ 6,\ 7,\ 11,\ 12,\ 14,\ 15,\ 19,\ 21,\ 22,\ 23,\ 24,\ 27,\ 28,\ 30,\ 31,\ \text{etc.}$$

ac propterea relinquuntur isti tantum:

$$1,\ 2,\ 4,\ 5,\ 8,\ 9,\ 10,\ 13,\ 16,\ 17,\ 18,\ 20,\ 25,\ 26,\ 29,\ 32,\ \text{etc.}$$

69. **Problema.** Si omnes numeri cubici $1,\ 2^3,\ 3^3,\ 4^3$ etc. per numerum quemcunque primum P dividantur, investigare indolem residuorum, quae inde nascentur.

Solutio. Sit a radix primitiva respectu divisoris primi P, et cum progressio geometrica $1,\ a,\ a^2,\ a^3,\ a^4$ etc. seriem residuorum completam exhibeat, quilibet numerus x per P divisus idem dabit residuum, quod quaepiam potestas ipsius a, quae sit a^λ. Hinc ejus numeri cubus x^3 idem dabit residuum quod potestas $a^{3\lambda}$, unde ex cubis eadem nascentur residua, atque ex progressione geometrica

$$1,\ a^3,\ a^6,\ a^9,\ a^{12},\ a^{15}\ \text{etc.}$$

ac sumto λ ita, ut 3λ sit vel $P-1$, vel ejus multiplum, potestas $a^{3\lambda}$ unitatem relinquet. Quare si pro λ minimus numerus accipiatur, cujus triplum sit per $P-1$ divisibile, numerus λ simul multitudinem omnium residuorum diversorum, quae ex divisione cuborum resultare possunt, indicabit.

Cum jam omnis numerus primus sit vel formae $3n+1$, vel $3n+2$, pro utraque forma judicium seorsim est instituendum.

I. Sit ergo $P=3n+1$, et quia $P-1=3n$, fiet $\lambda=n$, et residua cuborum omnia ex hac progressione geometrica nascentur:

$$1,\ a^3,\ a^6,\ a^9\ \ldots\ldots\ldots\ a^{3n-3}$$

quia sequens terminus a^{3n} iterum unitatem producit. Hinc non plures quam n numeri in residuis occurrent, ac reliqui duplo plures excluduntur, eruntque non-residua.

II. Si divisor primus sit $P=3n+2$, ideoque $P-1=3n+1$, minor numerus pro λ accipi nequit, quam $\lambda=3n+1$, ut 3λ per $P-1$ fiat divisibile, unde omnia residua diversa ex hac progressione geometrica nascentur:

$$1,\ a^3,\ a^6,\ a^9\ \ldots\ldots\ldots\ a^{9n},$$

quorum numerus cum sit $=3n+1$, in residuis omnes plane numeri divisore P minores occurrent, nullique excluduntur, seu nulla dabuntur non-residua.

70. **Coroll. 1.** Si ergo divisor primus P fuerit formae $3n+1$, cujusmodi numeri sunt:

$$7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97,\ \text{etc.}$$

in residuis cuborum tantum n numeri diversi occurrunt, indeque $2n$ numeri excluduntur.

71. **Coroll. 2.** Quare si haec cuborum progressio

$$1,\ 2^3,\ 3^3,\ 4^3\ \ldots\ldots\ (3n)^3,$$

unde omnia residua diversa prodire debent, per numerum primum $3n+1$ dividantur, quia terminorum numerus est $=3n$, quodlibet residuum ter occurrat necesse est, seu semper terni cubi minores quam $(3n)^3$, exhiberi possunt, qui idem residuum producant.

72. **Scholion 1.** Respectu ergo cuborum numeri primi formae $3n+1$ praecipue notari merentur, operaeque pretium erit residua in casibus simplicioribus notasse:

Divisor primus $3n+1$	1,	2^3,	3^3,	4^3,	5^3,	6^3,	7^3,	8^3,	9^3,	10^3,	11^3,	12^3,	13^3.	14^3,	15^3,	16^3,	17^3,	18^3	
	Residua																		
7	1,	1,	−1,	1,	−1,	−1,	0												
13	1,	−5,	1,	−1,	−5,	−5,	5,	5,	1,	−1,	5,	−1,	0						
19	1,	8,	8,	7,	−8,	7,	1,	−1,	7,	−7,	1,	−1,	−7,	8,	−7,	−8,	−8,	−1,	0

ubi manifesto quodvis residuum ter occurrit, totiesque idem signo — affectum: cujus ratio inde est perspicua, quod postremus cujusque ordinis cubus $(3n)^3$ pro residuo dat -1, et producta ex binis residuis semper quoque inter residua reperiantur. Cum igitur praeter cubum $(3n)^3$ semper dentur duo minores pariter residuum -1 habentes, qui sint f^3 et g^3, erunt formulae $1+f^3$ et $1+g^3$ per $3n+1$ divisibiles, et quia neque $1+f$ neque $1+g$ divisionem admittit, necesse est, ut hae $1-f+ff$ et $1-g+gg$ sint divisibiles; ubi quidem observare licet semper esse debere $g=-ff$, vel $g=m(3n+1)-ff$, quia tum fit $1+g^3=1-f^6$, quae aeque ac $1+f^3$ est divisibilis.

73. **Scholion 2.** Sint f^3, g^3, h^3 terni cubi minores quam $(3n+1)^3$, qui per numerum primum $3n+1$ divisi idem relinquant residuum, et quia binorum differentiae g^3-f^3, h^3-f^3 et h^3-g^3 divisionem admittunt, dum factores $g-f$, $h-f$, $h-g$ divisore sunt minores, hae tres formae $ff+fg+gg$, $ff+fh+hh$, $gg+gh+hh$ singulae per $3n+1$ divisibiles sint necesse est, hincque etiam binarum differentiae $hh-gg+fh-fg=(h-g)(f+g+h)$. Unde patet quoque summam radicum $f+g+h$ per divisorem $3n+1$ esse divisibilem: quae proprietas illi est analoga, qua invenimus si bina quadrata ff et gg per numerum quempiam primum P divisa idem residuum relinquant, dum ambo sunt minora quam P^2, tum summam radicum $f+g$ per P esse divisibilem. Pro casu nostro trium cuborum erit quoque

$$h(ff+fg+gg)-g(ff+fh+hh)=ff(h-g)-gh(h-g)$$

ideoque formula $ff-gh$ per $3n+1$ divisibilis, similique modo $gg-fh$ et $hh-fg$; hinc istas duas formulas ab illa $gg+gh+hh$ auferendo relinquitur haec $fg+fh+gh$ pariter per $3n+1$ divisibilis; et haec combinatio $(ff+fg+gg)+(hh-fg)$ praebet hanc $ff+gg+hh$ itidem per $3n+1$ divisibilem. Quocirca hoc habebimus theorema satis memorabile:

74. **Theorema.** Si f^3, g^3, h^3 fuerint terni cubi minores quam $(3n+1)^3$, qui per numerum primum $3n+1$ divisi idem relinquant residuum, tum sequentes formulae

$$f+g+h,\quad fg+fh+gh,\quad ff+gg+hh$$

singulae divisionem per $3n+1$ admittent.

75. **Coroll.** Ita pro divisore 19 videmus hos tres cubos 4^3, 6^3 et 9^3 idem residuum 7 dare; unde ob $f = 4$, $g = 6$, $h = 9$ fit $f + g + h = 19$, $fg + fh + gh = 114 = 6 . 19$ et $ff + gg + hh = 133 = 7 . 19$.

76. **Theorema.** Semper numeri hujus formae $pp + 3qq$ exhiberi possunt per numerum primum hujus formae $3n + 1$ divisibiles. At vero nulla ejusmodi datur formula $pp + 3qq$, quae per ullum numerum primum hujus formae $3n - 1$ sit divisibilis.

Demonstratio. Si $3n + 1$ sit numerus primus, tum tres adeo cubi f^3, g^3, h^3, quorum radices ipso sunt minores, exhiberi possunt, qui per $3n + 1$ divisi idem residuum relinquant, unde $g^3 - f^3$ per $3n + 1$ divisionem admittet, hincque etiam $ff + fg + gg$. At haec forma est vel $(f + \frac{1}{2}g)^2 + 3(\frac{1}{2}g)^2$, si g sit numerus par, vel $(\frac{1}{2}f + g)^2 + 3(\frac{1}{2}f)^2$, si f sit par, vel $\left(\frac{f-g}{2}\right)^2 + 3\left(\frac{f+g}{2}\right)^2$, si ambo sint impares, unde forma $ff + fg + gg$ semper ad hanc $pp + 3qq$ reducitur.

At si $3n - 1$ sit divisor primus, omnes cubi, quorum radices ipso sunt minores, diversa praebent residua, neque ergo binorum differentia, vel numerus hujus formae $ff + fg + gg$ exhiberi potest, qui per $3n - 1$ dividi posset; quod proinde etiam de numeris hujus formae $pp + 3qq$ locum habet. Atque hoc adeo de omnibus numeris formae $3n - 1$ valet, quoniam si non fuerint primi, factorem saltem primum istius formae involvunt.

77. **Coroll. 1.** Si igitur forma $pp + 3qq$ per numerum primum $3n + 1$ sit divisibilis, et quadratum qq per eundem divisum relinquat residuum γ, alterum quadratum pp relinquet residuum -3γ. Unde si omnes numeri quadrati per numerum primum $3n + 1$ dividantur, in residuis certe reperietur -3, vel $3n - 2$.

78. **Coroll. 2.** Sin autem omnes numeri quadrati per numerum primum formae $3n - 1$ dividantur, in serie residuorum certe non erit numerus -3; ideoque -3, vel $3n - 4$ erit non-residuum.

79. **Scholion.** Hinc si numeri quadrati per numerum quemcunque primum dividantur, de binis numeris $+3$ et -3 judicari poterit, utrum in ordine residuorum an non-residuorum occurrant. Omnes enim numeri primi praeter 2 et 3, qui hic non spectantur, in aliqua harum quatuor formarum continentur:

$$12m + 1, \quad 12m + 5, \quad 12m + 7, \quad 12m + 11,$$

quas singulas contemplemur.

I. Si divisor primus sit formae $12m + 1$, quatenus haec forma est $4n + 1$, tam $+1$ quam -1 erit residuum; quatenus vero est $3n + 1$, residuum quoque erit -3, hincque etiam $+3$. Hoc ergo in ordine residuorum occurrent $+3$ et -3.

II. Si divisor primus sit formae $12m + 5$, quatenus haec forma est $4n + 1$, in residuis erunt $+1$ et -1; quatenus vero est $3n - 1$, in residuis non reperitur -3, seu -3 erit non-residuum, hincque etiam $+3$. Quare hoc casu neuter numerorum $+3$ et -3 inter residua reperietur.

III. Si divisor primus sit formae $12m + 7$, quatenus haec forma est $4n - 1$, erit -1 non-residuum, quatenus vero est $3n + 1$, erit -3 residuum, ideoque $+3$ non-residuum. Unde hoc casu erit -3 residuum, at $+3$ non-residuum.

IV. Si divisor primus sit formae $12m+11$, quatenus haec forma est $4n-1$, erit -1 non-residuum, quatenus vero est formae $3n-1$, erit quoque -3 non-residuum, unde $+3$, utpote productum ex duobus non-residuis, inter residua occurret. Quare hoc casu erit $+3$ residuum, at -3 non-residuum.

Ad hanc ergo egregiam proprietatem consideratio cuborum nos perduxit, quae via cum satis sit obliqua, alia magis naturalis maxime desideratur.

80. **Problema.** Si omnes potestates quartae per numerum quemcunque primum P dividantur, investigare indolem residuorum, quae inde nascentur.

Solutio. Posita a radice primitiva respectu divisoris P, ut a^{P-1} sit infima potestas unitatem relinquens, ac residua quaesita orientur quoque ex hac progressione geometrica $1, a^4, a^8, a^{12}, a^{16}$ etc. eousque continuanda, donec exponens per $P-1$ fiat divisibilis, quod si eveniat in exponente 4λ, erit λ multitudo residuorum.

I. Sit divisor primus $P=4n+1$, ut sit $P-1=4n$; unde ut 4λ per $4n$ dividi queat, erit $\lambda=n$, hocque casu residua quaesita omnia ex hac progressione geometrica nascentur

$$1,\ a^4,\ a^8,\ a^{12}\ldots\ldots\ a^{4n-4},$$

quorum multitudo est n.

II. Sit divisor primus $P=4n+3$, ut sit $P-1=4n+2$; unde sumi debet $\lambda=2n+1$, et haec progressio geometrica

$$1,\ a^4,\ a^8,\ a^{12}\ldots\ldots\ a^{8n}$$

dabit omnia residua quaesita; cum autem a^{4n+2} unitatem relinquat uti a^0, termini

$$a^{4n+4},\quad a^{4n+8},\quad a^{4n+12}\ \text{etc.}$$

eadem residua praebent atque a^2, a^6, a^{10} etc. unde his interpolatis oritur progressio

$$1,\ a^2,\ a^4,\ a^6,\ a^8\ldots\ldots\ a^{8n},$$

quae eadem residua dat, ac progressio numerorum quadratorum. Ex biquadratis ergo hoc casu eadem plane residua omnia nascuntur atque ex ipsis quadratis.

81. **Coroll. 1.** Si ergo numeri biquadrati per numerum primum formae $4n+1$ dividantur, tantum n residua diversa oriuntur, unde semper quaterna biquadrata dantur p^4, q^4, r^4, s^4, quorum radices divisore sunt minores, quae per $4n+1$ divisa idem praebeant residuum; ubi quidem perspicuum est fore $s=-p$ et $r=-q$, seu quod eodem redit $s=4n+1-p$ et $r=4n+1-q$. Hinc istae formulae $p+q+r+s$, $p^2+q^2+r^2+s^2$ et $p^3+q^3+r^3+s^3$ per $4n+1$ erunt divisibiles.

82. **Coroll. 2.** Quaterna ergo biquadrata, quae per numerum primum $4n+1$ divisa unitatem relinquent, erunt valores ipsius x, quibus formula x^4-1 per $4n+1$ fit divisibilis, unde primo est $x=1$, tum si alius valor sit $x=b$, erit quoque $x=b^2$ et $x=b^3$; neque ultra progredi opus est, quia b^4 unitati aequivalet.

83. **Coroll. 3.** Cum potestas a^{2n} per $4n+1$ residuum det -1, patet si n sit numerus par, in residuis biquadratorum semper reperiri -1, et quodvis residuum quoque signo $-$ affectum occurrere; quod ergo evenit, si divisor primus sit formae $8m+1$; sin autem sit formae $8m+5$ tum -1 erit non-residuum.

84. **Coroll. 4.** Si ergo divisor primus sit formae $8m+1$, pro quovis biquadrato b^4 semper dabitur aliud p^4, ut summa b^4+p^4 sit per $8m+1$ divisibilis, atque adeo quaterna hujusmodi biquadrata p^4 assignari poterunt, quorum radices divisore sint minores; sin autem divisor sit formae $8m+5$, tum nulla summa binorum biquadratorum per eum divisibilis exhiberi potest.

85. **Scholion.** Cum summa binorum biquadratorum sit $b^4+p^4=(bb-pp)^2+2(bp)^2$, itemque $b^4+p^4=(bb+pp)^2-2(bp)^2$, pro quovis divisore primo formae $8m+1$ numeri tam hujus formae $xx+2yy$ quam hujus $xx-2yy$ exhiberi possunt per $8m+1$ divisibiles, unde si numeri quadrati per talem numerum primum $8m+1$ dividantur, in residuis occurrent numeri $+2$ et -2. Cum igitur demonstrari possit, numeros hujus formae $xx+2yy$ alios divisores non admittere, nisi qui ipsi sint ejusdem formae, hinc sequitur, omnes numeros primos formae $8m+1$ simul in forma $xx+2yy$ contineri. Quod est insigne theorema Fermatii, cujus demonstrationem nunc primum mihi eruere contigit. Huic autem aliud affine Fermatius proposuit, quod etiam omnes numeri primi hujus formae $8m+3$ in eadem forma $xx+2yy$ contineantur, cujus demonstrationem ex hac speculatione petere non licet, sequentem ergo ab amico mecum communicatam hic apponam.

86. **Theorema.** Nullus numerus hujus formae $2pp-qq$, siquidem p et q sint numeri inter se primi, ullum admittit divisorem sive hujus formae $8m+3$, sive hujus $8m-3$.

Demonstratio. Si numerorum p et q ambo sint impares, numerus $2pp-qq$ habebit formam $8n+1$; sin p sit par et q impar, formam habebit $8n-1$; sin autem p sit impar et q par $=2r$, forma erit $2(pp-2rr)$, ideoque vel $2(8n+1)$, vel $2(8n-1)$; semissis vero $pp-2rr$ iterum in forma $2pp-qq$ continetur, cum sit $pp-2rr=2(p+r)^2-(p+2r)^2$. Hoc praemisso si forma $2pp-qq$ divisorem haberet $8m\pm3$, per eundem divisibilis esset numerus formae $8n\pm1$, quotusque ergo foret iterum formae $8m\pm3$, atque minor divisore, quoniam p et q non solum divisore, sed etiam ejus semisse minores statuere licet. Cum igitur forma $2pp-qq$ per quotum, ideoque numerum minorem formae $8m\pm3$ esset divisibilis, ubi iterum p et q infra ejus semissem deprimere licet, quotus denuo minor divisore oriretur, et numeri p et q semper primi inter se manerent, ita ut neuter unquam ad nihilum redigeretur. Tandem ergo ad numerum minimum formae $2pp-qq$ perveniretur, qui foret per numerum formae $8m\pm3$, hoc est vel 3, vel 5 divisibilis, quod autem fieri non posse per se est perspicuum.

87. **Coroll. 1.** Quodsi ergo omnes numeri quadrati per divisores primos formae $8m\pm3$ dividantur, in residuis certe non occurret $+2$, quia alioquin ejusmodi forma $2pp-qq$ divisibilis exhiberi posset: ideoque pro talibus divisoribus erit $+2$ non-residuum.

88. **Coroll. 2.** Pro divisoribus autem primis formae $8m+3$ etiam -1 est non-residuum; unde cum producta ex binis non-residuis quadratorum transeant in residua, inter residua certe reperietur -2, hincque semper numeri formae $2pp+qq$ exhiberi poterunt per numerum primum $8m+3$ divisibiles, ex quo numerus primus $8m+3$ ipse ejusdem formae $2pp+qq$ sit necesse est, quod est alterum theorema Fermatii.

89. **Coroll. 3.** Pro divisoribus autem primis formae $8m-3$, in residuis quadratorum reperitur -1, unde cum productum ex residuo in non-residuum sit non-residuum, tam $+2$ quam

— 2 erunt non-residua; ideoque neutra harum formarum $2pp + qq$ et $2pp - qq$ unquam erit divisibilis per ullum numerum primum formae $8m - 3$.

90. **Scholion 1.** Eodem modo demonstrari potest nullum numerum formae $2pp + qq$, quoniam hujusmodi numeri omnes sunt vel $8n + 1$, vel $8n + 3$, per ullos numeros formae vel $8m - 1$, vel $8m - 3$ esse divisibiles, quoniam quoti ejusdem forent formae, et cum sint divisore minores, perveniendum esset ad minores numeros $2pp + qq$, qui forent per $8n - 1$, vel $8n - 3$, hoc est per 7 vel 5 divisibiles, quod autem evenire nequit. Hinc porro sequitur pro divisoribus primis formae $8m - 1$, vel $8m - 3$ necessario esse -2 non-residuum: ideoque pro divisoribus $8m - 1$ erit $+2$ residuum, et pro divisoribus $8m - 3$ non-residuum. Quod autem pro divisoribus primis formae $8m + 1$ tam $+2$ quam -2 in residuis quadratorum occurrant, simili ratiocinio vix ostendi posse videtur.

91. **Scholion 2.** Quae hactenus de residuis quadratorum sunt eruta, utrum numeri ± 2, ac supra etiam ± 3 in iis occurrant, nec ne? ita conspectui exposuisse juvabit:

Divisor primus		Divisor primus	
$4n + 1$	$+1$ residuum	$4n - 1$	$+1$ residuum
	-1 residuum		-1 non-residuum
$8n + 1$	$+2$ residuum	$8n - 1$	$+2$ residuum
	-2 residuum		-2 non-residuum
$8n + 3$	$+2$ non-residuum	$8n - 3$	$+2$ non-residuum
	-2 residuum		-2 non-residuum
$12n + 1$	$+3$ residuum	$12n - 1$	$+3$ residuum
	-3 residuum		-3 non-residuum
$12n + 5$	$+3$ non-residuum	$12n - 5$	$+3$ non-residuum
	-3 non-residuum		-3 residuum

Hinc per inductionem ulterius progredi licet hoc modo:

erit	si divisor primus sit
$+5$ residuum -5 residuum	$20n + 1$, $20n + 9$
$+5$ residuum -5 non-residuum	$20n - 1$, $20n - 9$
$+5$ non-residuum -5 residuum	$20n + 3$, $20n + 7$
$+5$ non-residuum -5 non-residuum	$20n - 3$, $20n - 7$
$+7$ residuum -7 residuum	$28n + 1$, -3, $+9$

erit	si divisor primus
$+7$ residuum -7 non-residuum	$28n-1,\ +3,\ -9$
$+7$ non-residuum -7 residuum	$28n+11,\ +15,\ +23$
$+7$ non-residuum -7 non-residuum	$28n+5,\ +13,\ +17$
$+11$ residuum -11 residuum	$44n+1,\ +9,\ +25,\ +5,\ +37$
$+11$ residuum -11 non-residuum	$44n-1,\ -9,\ -25,\ -5,\ -37$
$+11$ non-residuum -11 residuum	$44n+3,\ +15,\ +23,\ +27,\ +31$
$+11$ non-residuum -11 non-residuum	$44n+13,\ +17,\ +21,\ +29,\ +41$

quorum theorematum demonstrationes scientiam numerorum haud mediocriter promoverent.

92. **Theorema.** Si omnium numerorum potestates exponentis λ scilicet

$$1,\ 2^\lambda,\ 3^\lambda,\ 4^\lambda,\ 5^\lambda,\ 6^\lambda \text{ etc.}$$

per numerum primum formae $\lambda n+1$ dividantur, multitudo residuorum diversorum erit $=n$, ideoque multitudo non-residuorum $=(\lambda-1)n$.

Demonstratio. Sit a radix primitiva pro divisore primo $\lambda n+1$, cujus ergo potestates omnia plane suppeditant residua, et quilibet numerus divisore minor x erit residuum certae potestatis a^m, unde ejus potestas x^λ idem praebebit residuum quod $a^{\lambda m}$, quare omnia residua quaesita oriuntur ex hac progressione geometrica:

$$1,\ a^\lambda,\ a^{2\lambda},\ a^{3\lambda},\ a^{4\lambda} \ldots\ldots a^{(n-1)\lambda}$$

quoniam potestas sequens $a^{\lambda n}$ per numerum primum $\lambda n+1$ divisa iterum unitatem relinquit, eaque est minima hoc praestans; ex quo multitudo residuorum inde resultantium est $=n$, et cum multitudo omnium numerorum divisore minorum sit $=\lambda n$, reliquorum ex serie residuorum exclusorum multitudo erit $=(\lambda-1)n$.

93. **Coroll. 1.** Quare si series potestatum $1,\ 2^\lambda,\ 3^\lambda,\ 4^\lambda$ etc. usque ad $(\lambda n)^\lambda$ continuetur, in ea semper totidem termini, quot exponens λ continet unitates, reperientur, qui per numerum primum $\lambda n+1$ divisi idem residuum relinquant. Totidem ergo erunt qui unitatem relinquunt, ac si unius radix sit $=r$, reliquorum radices erunt

$$r^2,\ r^3,\ r^4 \ldots\ldots r^{\lambda-1}.$$

94. **Coroll. 2.** Semper ergo plures hujusmodi numerorum formae $p^\lambda-q^\lambda$ exhiberi possunt per numerum primum $\lambda n+1$ divisibiles, ita ut factor $p-q$ non sit divisibilis; atque adeo alterum numerorum p et q pro lubitu accipere licet.

95. **Coroll. 3.** Si n sit numerus par, in progressione geometrica 1, a^{λ}, $a^{2\lambda}$ etc. occurret terminus $a^{\frac{n}{2}\lambda}$, cui residuum -1 respondet; quare si divisor primus sit $2m\lambda + 1$, in residuis reperietur -1, sin autem sit $(2m + 1)\lambda + 1$, tum -1 erit non-residuum: evidens autem est si λ sit numerus impar, posteriorem formam locum habere non posse.

96. **Scholion 1.** Si omnes numerorum potestates quintae 1, 2^5, 3^5, 4^5 etc. per numeros primos formae $5n + 1$ qui sunt: 11, 31, 41, 61, 71 etc. dividantur, tantum n residua diversa resultabunt, inter quae utique reperietur -1. Hujusmodi ergo numerorum formae $p^5 \pm q^5$ dabuntur per numerum primum $5n + 1$ divisibiles, ita factor $p \pm q$ divisionem non admittat. Hinc alter factor, qui est $p^4 \mp p^3 q + p^2 q^2 \mp pq^3 + q^4$ per eundem erit divisibilis, qui cum sit

$$(pp + \tfrac{1}{2}pq + qq)^2 - 5(\tfrac{1}{2}pq)^2,$$

dabitur hujusmodi forma $ff - 5gg$ per $5n + 1$ divisibilis; unde sequitur si quadrata dividantur per numerum primum formae $5n + 1$, tum inter residua certe reperiri $+5$, quod cum conjectura ante allata congruit.

97. **Scholion 2.** Simili modo si potestates septimae per numerum primum $7n + 1$ dividantur, dabuntur hujusmodi formae $p^7 - q^7$, seu $p^6 + p^5 q + p^4 q^2 + p^3 q^3 + p^2 q^4 + pq^5 + q^6$ per eum divisibiles; haec vero expressio reducitur ad hanc formam:

$$(p^3 + \tfrac{1}{2}ppq - \tfrac{1}{2}pqq - q^3)^2 + 7(\tfrac{1}{2}ppq + \tfrac{1}{2}pqq)^2.$$

Unde semper numeri hujus formae $ff + 7gg$ exhiberi possunt per numerum primum $7n + 1$ divisibiles. Ex quo sequitur si omnia quadrata per numerum primum formae $7n + 1$ dividantur, inter residua certe repertum iri -7, quo etiam conjectura supra data confirmatur.



XXXVIII.

Novae demonstrationes circa resolutionem numerorum in quadrata.

(Acta Erudit. Lips. 1773 p. 193. Acta Petrop. I. II. 1775 p. 48. Exhib. 1772. Sept. 21.)

1. Quum saepe et multum in hoc argumento occupatus fuissem, neque tamen ea demonstratio, quam olim dederam circa resolutionem omnium numerorum in quatuor vel pauciora quadrata, mihi ipsi penitus satisfecisset: eo majore ardore evolvi demonstrationem, quam Celeb. D. La Grange nuper in primo volumine Novorum Actorum Acad. sç. Boruss. hujus theorematis tradidit, quam utique negotium perfecisse sum admiratus, etiamsi ejus momenta nimis longe repetita et vehementer operosa viderentur.

2. Lectoribus autem haud ingratum fore arbitror, si praecipua momenta, quibus haec demonstratio innititur, hic breviter et concinne proposuero. Postquam Cel. Auctor hoc praemisit lemma, quod si duae summae binorum quadratorum $pp+qq$ et $rr+ss$ communem habeant divisorem ϱ, neque tamen singula quadrata per eum dividi queant, tum non solum ipsum hunc divisorem ϱ, sed etiam ambos quotos $\frac{pp+qq}{\varrho}$ et $\frac{rr+ss}{\varrho}$ fore summas duorum quadratorum: progreditur ad hoc theorema demonstrandum: *quod si summa quatuor quadratorum* $P^2+Q^2+R^2+S^2$ *divisibilis fuerit per numerum quemcunque* A, *neque tamen singula quadrata per eum sint divisibilia, tum ipsum hunc numerum* A *fore summam quatuor quadratorum*, cujus demonstratio sequentibus continetur ratiociniis:

I. Posito quoto ex illa divisione oriundo $=a$, ut sit $Aa=P^2+Q^2+R^2+S^2$, si forte eveniat, ut binae formulae P^2+Q^2 et R^2+S^2 habeant communem divisorem ϱ, quem ergo etiam numerus a continebit, ponit $a=b\varrho$, ut fiat $Ab=\frac{P^2+Q^2}{\varrho}+\frac{R^2+S^2}{\varrho}$, quae formulae cum per lemma praemissum sint summae duorum quadratorum, habebitur hujusmodi aequatio:

$$Ab=pp+qq+rr+ss,$$

ubi formulae $pp+qq$ et $rr+ss$ non amplius habebunt factorem communem.

II. Tum vero ponit $pp+qq=t$ et $rr+ss=u$, ut sit $Ab=t+u$, quam aequationem ducit in t, faciendo $Abt=tt+tu$, et quia tu etiam est summa duorum quadratorum, puta $xx+yy$, sumendo scilicet $x=pr+qs$ et $y=ps-qr$, fiet $Abt=tt+xx+yy$.

III. Nunc per numeros t et b, quippe qui inter se sunt primi, ambos x et y ita exprimi posse observat, ut sit $x=\alpha t+\gamma b$ et $y=\beta t+\delta b$, ubi cum litterae α, β, γ, δ infinitis modis accipi queant, sive negative, sive positive, inter earum valores certe tales dabuntur, ut sit $\alpha<\frac{1}{2}b$ et $\beta<\frac{1}{2}b$.

IV. His jam valoribus pro x et y substitutis, resultabit ista aequatio:

$$Abt = tt(1 + \alpha\alpha + \beta\beta) + 2bt(\alpha\gamma + \beta\delta) + bb(\gamma\gamma + \delta\delta),$$

quae expressio cum divisibilis esse debeat per b, neque tamen in primo membro tt hanc divisionem admittat, necesse est, ut ibi formula $1 + \alpha\alpha + \beta\beta$ factorem habeat b; eodem modo etiam in ultimo membro factorem $\gamma\gamma + \delta\delta$ divisibilem per t esse necesse est. Ponatur ergo $1 + \alpha\alpha + \beta\beta = ba'$, et quia uterque numerus α et β minor est quam $\frac{1}{2}b$, manifestum est fore $a' < \frac{1}{2}b + \frac{1}{b}$; facta ergo divisione per b, erit $At = a'tt + 2t(\alpha\gamma + \beta\delta) + b(\gamma\gamma + \delta\delta)$.

V. Multiplicetur nunc haec aequatio per a', ut prodeat

$$Aa't = a'^2tt + 2a't(\alpha\gamma + \beta\delta) + a'b(\gamma\gamma + \delta\delta)$$

et in ultimo membro, loco $a'b$ scribendo $1 + \alpha\alpha + \beta\beta$ fiet

$$Aa't = a'^2tt + 2a't(\alpha\gamma + \beta\delta) + (\alpha\alpha + \beta\beta)(\gamma\gamma + \delta\delta) + \gamma\gamma + \delta\delta,$$

quae expressio in sequentia quatuor quadrata resolvetur

$$Aa't = (a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2 + \gamma^2 + \delta^2,$$

ubi, cum summa binorum postremorum quadratorum $\gamma^2 + \delta^2$ divisibilis sit per numerum t, necesse est, ut summa duorum primorum quoque per t sit divisibilis, ita ut hic duae binorum quadratorum summae occurrant communem divisorem t habentes: quare si per t dividatur, ambo illi quoti itidem erunt summae binorum quadratorum.

VI. Quodsi ergo ponamus $\frac{(a't + \alpha\gamma + \beta\delta)^2 + (\beta\gamma - \alpha\delta)^2}{t} = p'^2 + q'^2$ et $\frac{\gamma^2 + \delta^2}{t} = r'^2 + s'^2$, habebimus $Aa' = p'p' + q'q' + r'r' + s's'$; in hac autem formula Aa', si cum prima Aa comparetur, numerus a' multo minor erit quam a, quandoquidem $b < a$ et $a' < \frac{1}{2}b$. Simili modo ergo pervenire licebit ad formulam Aa'', ubi a'' multo minor erit quam a'; sicque tandem perveniri necesse est ad formulam $A.1$, ita ut jam ipse numerus A reperiatur aequalis summae quatuor quadratorum.

3. Demonstrato hoc theoremate insuper ostendi oportet, proposito quocunque numero primo, semper exhiberi posse summam quatuor quadratorum per eum divisibilem, quorum tamen singula quadrata divisionem non admittant. Atque hoc etiam Cel. La Grange modo maxime ingenioso demonstrat, qui autem tantopere est abstrusus et prolixus, ut ejus momenta breviter et dilucide nequaquam exhiberi possint. Nunc igitur famosum illud theorema sive Bacheti, sive Fermatii, *quod omnis numerus in quadrata quatuor vel pauciora resolvi possit*, pro perfecte demonstrato est habendum, quia enim pro numero primo quocunque semper dari potest summa quatuor quadratorum, per illum divisibilis, omnes numeri primi summae erunt quatuor pauciorumve quadratorum; et quia jamdudum demonstratum est, producta ex duobus pluribusve numeris, qui singuli sunt summae quatuor pauciorumve quadratorum, etiam in quatuor quadrata dispertiri posse, solidissime jam est evictum, omnes plane numeros esse summas quatuor quadratorum pauciorumve.

4. Quamvis omnino nefas esset, quicquam contra soliditatem et rigorem harum demonstrationum excipere: tamen nemo negabit, eas nimis longe esse repetitas, neque ipsa fundamenta et rationes singulorum ratiociniorum, e quibus hae demonstrationes sunt compositae, haud levi obscuritate esse involutas, ita ut etiam nunc merito clariores et perceptu faciliores demonstrationes desiderare

liceat. Quo quidem desiderio, summae laudi, quam istae demonstrationes merentur, nihil detrahi est censendum.

5. Cum igitur postquam hoc argumentum de novo perpendissem, in novas et satis planas eorundem theorematum demonstrationes mihi incidere contigerit, iis, qui hoc studio delectantur, communicatio novarum harum demonstrationum certe gratissima fore videtur; quocirca eas hoc loco, quantum potero, dilucide breviterque sum propositurus. Ac primo quidem a theoremate illo notissimo simulque plenissime demonstrato, quo omnes divisores cujusque summae duorum quadratorum inter se primorum aequales affirmantur ipsi summae duorum quadratorum, incipiam; cum quod haec nova demonstratio simplicitate se maxime commendat, tum vero quod iisdem vestigiis insistendo demonstratio facile ad quatuor quadrata extendi potest.

6. **Lemma 1.** *Productum ex duobus summis binorum quadratorum itidem est summa duorum quadratorum.* Nam si illud productum fuerit e. g. $(aa+bb)(\alpha\alpha+\beta\beta)$, et capiatur

$$A = a\alpha + b\beta \text{ et } B = a\beta - b\alpha, \text{ utique erit } (aa+bb)(\alpha\alpha+\beta\beta) = AA + BB.$$

Theorema 1. Si numerus N fuerit divisor summae duorum quadratorum P^2+Q^2 inter se primorum, tum ipse ille numerus N erit summa duorum quadratorum.

Demonstratio. Quo hanc demonstrationem facilius etiam in numeris exsequi liceat, cui forte libuerit, observo, quantumvis magni fuerint numeri P et Q, ex iis semper aliam summam duorum quadratorum $pp+qq$ formari posse, quorum radices p et q semissem numeri propositi N non superent. Nam si ponatur $P = fN \pm p$ et $Q = gN + q$, notissimum est numeros p et q ita sumi posse, ut semissem $\frac{1}{2}N$ non superent; cum igitur jam sit

$$PP + QQ = NN(ff+gg) + 2N(\pm fp \pm gq) + pp + qq,$$

haecque expressio per N sit divisibilis, evidens est etiam hanc binorum quadratorum summam per N divisibilem fore. Hoc praemisso, ipsam demonstrationem sequentibus momentis complectar:

I. Cum ista formula $pp+qq$ divisorem habeat N, ponendo quotum $= n$, habebimus $Nn = pp+qq$, ubi ergo $n < \frac{1}{2}N$, quia $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$.

II. Jam istos numeros p et q per numerum n ita exprimere licebit, ut sit $p = a + \alpha n$ et $q = b + \beta n$, ubi admissis etiam numeris negativis pro a et b, eos infra $\frac{1}{2}N$ deprimere licebit, uti jam initio observavimus. Tum vero erit

$$Nn = aa + bb + 2n(a\alpha + b\beta) + nn(\alpha\alpha+\beta\beta),$$

et quia in lemmate praemisso erat $a\alpha + b\beta = A$, fiet $Nn = aa + bb + 2nA + nn(\alpha\alpha+\beta\beta)$.

III. Hujus ergo expressionis primum membrum $aa+bb$ factorem habeat necesse est n, quia reliqua membra jam per se divisorem n admittunt. Statuamus ergo $aa+bb = nn'$, et quia $a < \frac{1}{2}n$ et $b < \frac{1}{2}n$, ideoque $nn' < \frac{1}{2}nn$, erit utique $n' < \frac{1}{2}n$: Hoc autem valore substituto et divisione per n facta, prodit

$$N = n' + 2A + n(\alpha\alpha+\beta\beta).$$

IV. Hanc aequationem ducamus in n', et quia $nn' = aa+bb$, membrum postremum per lemma praemissum reducitur ad $nn'(\alpha\alpha+\beta\beta) = (aa+bb)(\alpha\alpha+\beta\beta) = AA+BB$; ita ut nunc habeamus $Nn' = n'n' + 2n'A + AA + BB$, quae expressio manifesto est summa duorum quadratorum, scilicet $Nn' = (n'+A)^2 + B^2$.

V. Cum ergo initio fuisset productum Nn summa duorum quadratorum, indeque hic elicuerimus productum minus Nn' etiam aequale summae duorum quadratorum, eodem modo ad talia producta continuo minora pertingere licebit, scilicet Nn'', Nn''' etc.; necesse igitur est, ut tandem ad productum minimum, scilicet $N.1$ perveniatur, sicque ipse numerus N propositus quoque erit summa duorum quadratorum.

Corollarium. Mirum forsitan videbitur, cum perventum fuerit ad hujusmodi numerum $n' = 1$. quomodo sequentes operationes similes se sint habiturae; id quod facile patebit sumendo statim $n = 1$, tum enim habebitur $p = a + \alpha.1$ et $q = b + \beta.1$, ubi manifesto sumere licet $a = 0$ et $b = 0$, quippe quo pacto fiunt $< \frac{1}{2}$; tum vero ob $aa + bb = 0$. utique erit $n' = 0$, atque hic progressio ulterior nostri ratiocinii sponte sistitur.

Scholion. Eodem modo demonstrari potest, omnes numeros, vel hujus formae $pp + 2qq$. vel $pp + 3qq$ alios non admittere divisores, nisi qui ipsi sint ejusdem formae, siquidem numeri p et q fuerint primi inter se. Neque vero hoc ratiocinium ad formas ulteriores, veluti $pp + 5qq$, $pp + 6qq$ extendi potest, quia tum non amplius sequeretur numerum n' necessario minorem esse quam n. Priorum igitur illorum casuum demonstrationes hic apponamus.

7. **Lemma 2.** *Productum ex duobus numeris hujus formae* pp + 2qq *semper est numerus ejusdem formae.* Si enim tale productum proponatur $(aa + 2bb)(\alpha\alpha + 2\beta\beta)$, et sumatur $A = a\alpha + 2b\beta$ et $B = a\beta - b\alpha$, tum utique erit $AA + 2BB = (aa + 2bb)(\alpha\alpha + 2\beta\beta)$.

Theorema 2. Si N fuerit divisor numeri $pp + 2qq$, et p et q sint primi inter se, tum etiam ipse numerus N in tali forma continebitur.

Demonstratio. Hic iterum numeros p et q infra semissem numeri N deprimere licebit, et nostra demonstratio sequenti modo procedet:

I. Sit $Nn = pp + 2qq$, at quia $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$, erit $n < \frac{3}{4}N$. Jam ponatur ut ante $p = a + \alpha n$ et $q = b + \beta n$, ubi a et b capi poterunt minores quam $\frac{1}{2}n$, hincque habebitur

$$Nn = aa + 2bb + 2n(a\alpha + 2b\beta) + nn(\alpha\alpha + 2\beta\beta).$$

quae forma per lemma praemissum reducitur ad

$$Nn = aa + 2bb + 2nA + nn(\alpha\alpha + 2\beta\beta).$$

II. Hic igitur primum membrum $aa + 2bb$ factorem habebit n, unde posito $aa + 2bb = nn'$, erit utique $n' < \frac{3}{4}n$: hoc jam valore substituto et per n diviso prodit $N = n' + 2A + n(\alpha\alpha + 2\beta\beta)$.

III. Multiplicetur per n', atque per praecedens lemma habebitur

$$nn'(\alpha\alpha + 2\beta\beta) = (aa + 2bb)(\alpha\alpha + 2\beta\beta) = AA + 2BB,$$

ita ut nunc habeatur $Nn' = n'n' + 2n'A + AA + 2BB$, quae manifesto ad hanc reducitur formam:

$$Nn' = (n' + A)^2 + 2BB,$$

ideoque itidem numerus formae $pp + 2qq$.

IV. Cum ergo sit $n' < n$, simili modo ad producta sequentia pervenire licebit, scilicet Nn'', Nn''' etc. ita ut numeri n, n', n'', n''' etc. continuo decrescant; tandem ergo perveniatur necesse est ad formam $N.1$, ita ut ipse numerus N quoque in forma eadem $pp + 2qq$ contineatur.

8. **Lemma 3.** *Productum ex duobus numeris formae* $pp + 3qq$ *semper ad similem formam reduci potest.* Sit enim tale productum $(aa + 3bb)(\alpha\alpha + 3\beta\beta)$ et capiatur $A = a\alpha + 3b\beta$ et $B = a\beta - b\alpha$, manifesto habebitur $AA + 3BB = (aa + 3bb)(\alpha\alpha + 3\beta\beta)$.

Theorema 3. Si N fuerit divisor numeri $pp + 3qq$, ubi p et q sint numeri primi inter se, tum ipse numerus N ad eandem formam reduci poterit.

Demonstratio. Cum iterum spectare liceat $p < \frac{1}{2}N$ et $q < \frac{1}{2}N$, ipsa forma $pp + 3qq$ minor erit quam N^2; posito ergo $pp + 3qq = Nn$, factor n minor erit quam N, quae quidem reductio ad demonstrationem non est necessaria: ea enim aeque procedet, etiamsi fuerit $n > N$, uti sequitur:

I. Posito jam $p = a + \alpha n$ et $q = b + \beta n$, hic numeros a et b minores statuere licet quam $\frac{1}{2}n$, saltem non majores. Tum autem erit $Nn = aa + 3bb + 2n(a\alpha + 3b\beta) + nn(\alpha\alpha + 3\beta\beta)$, quae per lemma praemissum fit

$$Nn = aa + 3bb + 2nA + nn(\alpha\alpha + 3\beta\beta).$$

II. Necesse igitur est, ut primum membrum $aa + 3bb$ factorem habeat n; quare posito $aa + 3bb = nn'$, hic numerus n' certe minor erit quam n, saltem non major, tum vero facta divisione per n prodibit

$$N = n' + 2A + n(\alpha\alpha + 3\beta\beta).$$

III. Multiplicemus jam per n', et postremum membrum

$$nn'(\alpha\alpha + 3\beta\beta) = (aa + 3bb)(\alpha\alpha + 3\beta\beta)$$

per lemma praecedens fit $AA + 3BB$; sicque habebimus $Nn' = n'n' + 2n'A + AA + 3BB$, quae expressio manifesto reducitur ad hanc:

$$Nn' = (n' + A)^2 + 3BB.$$

IV. Cum igitur Nn' iterum sit formae $pp + 3qq$ et $n' < n$, eodem modo continuo progredi licebit ad continuo minora producta Nn'', Nn''' etc. donec tandem ad ultimum $N.1$ perveniatur; atque adeo demonstrationem habemus, ipsum numerum N fore formae $pp + 3qq$.

Coroll. 1. Fundamentum hujus demonstrationis, ut et praecedentium, in hoc consistit, quod a quolibet numero n perveniatur ad alium n' multo minorem, id quod iis casibus, quibus n est numerus satis magnus, per se est perspicuum. Quin etiam haec ratio eo casu valet, quo $n = 1$; quia enim tum sumi poterit $a = 0$ et $b = 0$, tum ob $nn' = 0$ utique fiet $n' = 0$. Interim tamen pro hoc theoremate singularis plane casus occurrit, quando in progressione numerorum n, n', n'' etc. tandem ad binarium pervenitur; qui casus eo majorem attentionem meretur, quod nusquam alibi occurrat.

Coroll. 2. Pro hoc ergo casu statuamus statim $n = 2$, et manifestum est in formula $pp + 3qq$ utrumque numerum p et q esse debere imparem: utrumque enim parem assumere non licet, quia p et q primi inter se statuuntur; quare cum hic fieri debeat $p = a + 2\alpha$ et $q = b + 2\beta$, fiet $a = 1$ et $b = 1$, ideoque $aa + 3bb = 4 = nn'$, unde patet etiam fore $n' = 2$, ita ut nulla ulterior diminutio locum habere possit. Quoties ergo hoc evenit, tum non ipse numerus N, sed ejus duplum $2N$ erit numerus formae $pp + 3qq$.

Coroll. 3. Hoc eo magis clarum redditur, si perpendamus, formulam $pp+3qq$, quando ambo numeri p et q sunt impares, non solum esse parem, sed etiam per 4 divisibilem, neque unquam adeo impariter parem esse posse formam $pp+3qq$. Quoties ergo, uti in his casibus usu venit, numerus $2N$ in forma $pp+3qq$ contineatur, tum N semper erit numerus par, ejusque semissis $\frac{1}{2}N$, seu pars quarta ipsius $2N$ in hac forma $pp+3qq$ continebitur. Quoties enim uterque numerus p et q est impar, tum etiam $\frac{pp+3qq}{4}$ semper quoque est numerus ejusdem formae, idque adeo in integris, quod quidem non tam facile perspicitur; posito enim $p=2r+1$ et $q=2s+1$, prodit

$$\frac{pp+3qq}{4}=1+r+rr+3s+3ss,$$

quam generatim neutiquam in integris ad quadratum cum triplo quadrato reducere licet. Sequenti autem modo haec resolutio in genere institui poterit: primum scilicet observo, omnia quadrata imparia in hac forma $(4m+1)^2$ contineri, siquidem pro m etiam numeri negativi admittuntur; namque si m sit positivum, quadrata numerorum 1, 5, 9, 13, quorum forma est $4i+1$, resultant; si m negativum, quadrata numerorum 3, 7, 11, 15 etc., quorum forma est $4i-1$, oriuntur. Jam ponamus $pp=(4r+1)^2$ et $qq=(4s+1)^2$ eritque $\frac{pp+3qq}{4}=1+2r+4rr+6s+12ss$, quae manifesto ad hanc formam redigitur

$$(1+r+3s)^2+3(r-s)^2.$$

Scholion. His theorematibus praemissis, id quod nobis maxime est propositum aggrediamur, demonstraturi *quod summae quatuor quadratorum nullos alios divisores admittant, nisi qui ipsi sunt summae quatuor quadratorum.* Ad similitudinem autem praecedentium theorematum lemma quoque praemitti oportet.

9. **Lemma 4.** *Productum ex duobus pluribusve numeris, qui singuli sunt summae quatuor quadratorum semper quoque per summam quatuor quadratorum exprimi potest.* Sit tale productum

$$(aa+bb+cc+dd)(\alpha\alpha+\beta\beta+\gamma\gamma+\delta\delta)$$

et capiatur $A=a\alpha+b\beta+c\gamma+d\delta$, $B=a\beta-b\alpha-c\delta+d\gamma$, $C=a\gamma+b\delta-c\alpha-d\beta$, $D=a\delta-b\gamma+c\beta-d\alpha$, horumque quadratorum summa erit

$$A^2+B^2+C^2+D^2=(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2):$$

manifestum enim est, singula producta ex binis partibus se mutuo destruere, et singula quadrata litterarum latinarum in singula graecarum duci.

Theorema 4. Si N fuerit divisor cujuspiam summae quatuor quadratorum, seu formae $pp+qq+rr+ss$, quae quidem singula per N non sint divisibilia, tum N certe erit summa quatuor quadratorum.

Demonstratio. Non parum juvabit hic quoque notasse, quatuor illas radices p, q, r, s infra semissem numeri propositi N deprimi posse; demonstratio autem sequenti modo procedit:

I. Denotante n quotum ex illa divisione resultantem, ut sit $Nn=pp+qq+rr+ss$, ubi litterae p, q, r, s ita ad n referantur, ut sit $p=a+n\alpha$, $q=b+n\beta$, $r=c+n\gamma$, $s=d+n\delta$, evidens omnino est, litteras a, b, c, d ita sumi posse, ut $\frac{1}{2}n$ non superent, quandoquidem valores negativi hinc non excluduntur. Sicque formula $aa+bb+cc+dd$ certe minor erit quam nn.

II. His autem valoribus substitutis aequationem adipiscemur sequentem:

$$Nn = aa + bb + cc + dd + 2n(a\alpha + b\beta + c\gamma + d\delta) + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta),$$

quae ex lemmate praemisso, ubi posuimus $A = a\alpha + b\beta + c\gamma + d\delta$, contrahitur in

$$Nn = aa + bb + cc + dd + 2nA + nn(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

Quia ergo hic pars prima $aa + bb + cc + dd$ factorem habere debet n, statuatur

$$aa + bb + cc + dd = nn',$$

eritque omnino $n > n'$, sive $n' < n$, uti modo ostendimus. Facta ergo divisione per n obtinebimus

$$N = n' + 2A + n(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta).$$

III. Multiplicemus nunc per n', et quia $nn' = aa + bb + cc + dd$, habebimus ex lemmate

$$nn'(\alpha\alpha + \beta\beta + \gamma\gamma + \delta\delta) = A^2 + B^2 + C^2 + D^2,$$

qua forma introducta nostra aequatio fiet $Nn' = n'n' + 2n'A + A^2 + B^2 + C^2 + D^2$, quae ad haec quatuor quadrata manifesto reducitur $(n' + A)^2 + B^2 + C^2 + D^2 = Nn'$.

IV. Quatenus igitur hic $n' < n$, eodem modo ad formas continuo minores Nn'', Nn''' etc. pertingere licebit, donec tandem ad formam $N.1$ perveniatur, ideoque numerus propositus N quatuor quadratis aequetur.

Coroll. 1. Hoc ratiocinium iterum levi exceptioni est obnoxium quando $n = 2$, omnesque numeri p, q, r, s impares: tum enim fiet $a = 1$, $b = 1$, $c = 1$, $d = 1$, hincque $nn' = 4$, ita ut quoque fiat $n' = 2$, sicque non minor quam n. Verum cum hinc numerus $2N$ aequetur summae quatuor quadratorum, aliunde perspicuum est etiam semissem N fore summam quatuor quadratorum, ita ut haec exceptio nihil plane turbare sit censenda.

Coroll. 2. Quo hoc clarius perspiciatur, sint numeri p, q, r, s impares, et n numerus par; tum quia $Nn = pp + qq + rr + ss$, erit

$$\frac{1}{2}Nn = \left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2 + \left(\frac{r+s}{2}\right)^2 + \left(\frac{r-s}{2}\right)^2$$

quae quatuor quadrata itidem erunt integra; qua reductione uti licebit, quamdiu omnes radices quatuor quadratorum fuerint impares; tum autem exceptio ante memorata sponte concidit.

Scholion. Hac demonstratione potissimum theorema illud Fermatianum conficitur, quandoquidem altera pars, quae adhuc superest, quod scilicet proposito quocunque numero primo semper summae quatuor quadratorum exhiberi queant per illum divisibiles, a me jam dudum satis clare est expedita atque adeo nuper a Celeb. la Grange subtilissima demonstratione est firmata. Ut tamen hoc argumentum penitus conficiam, sequentem demonstrationem admodum facilem hic subjungam.

10. **Theorema 5.** Proposito quocunque numero primo N non solum quaterna, verum adeo terna quadrata infinitis modis exhiberi possunt, quorum summa sit divisibilis per istum numerum N, neque tamen singula per eum dividi queant.

Demonstratio. Respectu numeri N omnes plane numeri in aliqua sequentium formarum continentur:

$$\lambda N,\ \lambda N + 1,\ \lambda N + 2,\ \lambda N + 3, \ldots \lambda N + N - 1,$$

quarum numerus est N. Seposita autem prima forma, quae multipla ipsius λN continet, circa reliquas, quarum numerus est $N - 1$, notandum est, quadrata primae formae $\lambda N + 1$ et ultimae $\lambda N + N - 1$ ad eandem formam $\lambda N + 1$ redire; quadrata vero secundae formae $\lambda N + 2$ et penul-

timae $\lambda N + N - 2$ ad formam $\lambda N + 4$; tertiae vero et antepenultimae ad $\lambda N + 9$ redigi, et ita porro, ita ut hae tantum formae

$$\lambda N + 1, \quad \lambda N + 4, \quad \lambda N + 9, \text{ etc.},$$

quarum numerus est $\frac{1}{2}(N - 1)$, quadrata in se complecti queant, quas formas primae classis appellemus, et ita designemus:

$$\lambda N + a, \quad \lambda N + b, \quad \lambda N + c, \quad \lambda N + d, \text{ etc.},$$

ita ut litterae a, b, c, d, etc., vel ipsa quadrata 1, 4, 9, 16 denotent, vel, si numerum N excedant, residua ex divisione restantia. Reliquae vero formae, quarum numerus itidem erit $\frac{1}{2}(N - 1)$, hoc modo designentur:

$$\lambda N + \alpha, \quad \lambda N + \beta, \quad \lambda N + \gamma, \text{ etc.},$$

quas formas posterioris classis vocabimus. De his autem geminis classibus tres sequentes proprietates notentur, quas quidem facile demonstrare licet:

I. Productum ex binis numeris primae classis itidem in prima classe continetur, scilicet forma $\lambda N + ab$ in prima classe reperietur; si enim ab majus fuerit quam N, ejus loco residuum ex divisione per N facta relictum capi est intelligendum.

II. Numeri primae classis a, b, c, d, etc. in quemcunque numerum posterioris classis α, β, γ, etc. ducti, in classem posteriorem incident.

III. Denique producta ex binis numeris posterioris classis, veluti $\alpha\beta$, in classem primam transferuntur.

His praemissis demonstrabo: si non darentur terna quadrata, quorum summa divisibilis esset per N, tum maximum absurdum inde esse secuturum. Ad hoc concedamus tantisper adversario, nulla dari terna quadrata, quorum summa sit divisibilis per N: multo minus ergo duo talia quadrata dabuntur. Hinc statim sequitur, formam $\lambda N - a$, sive quod eodem redit $\lambda N + (N - a)$ non in prima classe occurrere: si enim daretur quadratum formae $\lambda N - a$, hoc ad quadratum formae $\lambda N + a$ praeberet summam per N divisibilem, contra hypothesin. Forma igitur $\lambda N - a$ in posteriore classe contineatur necesse est, sicque inter litteras α, β, γ, δ, etc. reperientur numeri -1, -4, -9, etc. Sit f numerus quicunque primae classis, ita ut dentur quadrata formae $\lambda N + f$, ad quae si addantur quadrata formae $\lambda N + 1$, summa binorum habebit formam $\lambda N + f + 1$. Jam si daretur quadratum formae $\lambda N - f - 1$, haberetur summa trium quadratorum per N divisibilis, quod cum negetur, forma $\lambda N - f - 1$ non in prima classe, ideoque in posteriori continebitur, in qua ergo quum reperiantur numeri -1 et $-f - 1$, eorum productum $+f + 1$ in priori classe occurrat necesse est. Simili modo ostendetur in prima classe quoque occurrere debere numeros

$$f + 2, \quad f + 3, \quad f + 4, \text{ etc.}$$

quare sumto $f = 1$, in prima classe occurrerent omnes plane formae

$$\lambda N + 1, \quad \lambda N + 2, \quad \lambda N + 3, \text{ etc.}$$

nullaeque penitus pro classe posteriore relinquerentur. Interim tamen eodem ratiocinio vidimus, in classe posteriore occurrere numeros -1, $-f - 1$, $-f - 2$, etc. ideoque etiam omnes plane formas; quod cum sit maxime absurdum, sequitur falsum esse, non dari terna quadrata, quorum

summa sit divisibilis per numerum propositum N. Dantur ergo omnino terna multoque magis quaterna hujusmodi quadrata, quorum summa per N erit divisibilis.

Corollarium. Ex hoc theoremate cum praecedente conjuncto manifesto sequitur, omnes plane numeros primos esse summas quatuor vel pauciorum quadratorum. Et quum producta ex binis pluribusve hujusmodi numeris eandem naturam sequantur, solidissime evictum est, *omnes plane numeros esse summas quatuor quadratorum vel adeo pauciorum.*

Scholion. Loco hujus propositionis Cel. La Grange theorema multo latius patens in medium attulit et demonstratione munivit ingeniosissima quidem, sed tantopere abstrusa et intellectu difficili, ut non nisi summa adhibita attentione percipi posset. Demonstravit scilicet, proposito quocunque numero primo A semper bina quadrata pp et qq ad illum prima dari posse, ita ut formula $pp - Bqq - C$ per eum numerum primum A fiat divisibilis, quicunque numeri pro litteris B et C accipiantur, dummodo fuerint primi respectu ipsius A. Idem igitur theorema aliquanto latius extensum cum demonstratione longe faciliori et planiori hic subjungam.

11. **Theorema 6.** Proposito quocunque numero primo N, semper terna quadrata xx, yy et zz ad eum prima exhibere licet, ut formula $\lambda xx + \mu yy + \nu zz$ per numerum illum primum N fiat divisibilis, dummodo isti coefficientes λ, μ et ν ad ipsum N fuerint primi, hoc est, nullus eorum neque evanescat, neque ipsi N, neque ejus multiplo cuipiam fuerit aequalis.

Demonstratio. Denotent litterae a, b, c, d, etc. omnia residua, quae ex divisione quadratorum per numerum primum propositum N facta relinquuntur, quos numeros ante ad classem priorem retulimus, quorum multitudo est $\frac{1}{2}(N-1)$: in iis scilicet omnes occurrunt numeri quadrati 1, 4, 9, 16, etc. minores quam N; majorum autem residua illa ex divisione per N resultantia accedunt. Ad eandem vero classem etiam iidem numeri a, b, c, d, etc. quovis multiplo numeri N aucti sunt referendi. Omnes autem reliqui numeri minores quam N, quorum numerus itidem est $\frac{1}{2}(N-1)$, quosque non-residua appellare licet, ad classem posteriorem sunt relati et litteris graecis α, β, γ, δ, etc. designentur. Circa hos numeros duplicis generis jam ante notavimus, producta ex binis residuis, seu classis prioris, iterum in eandem classem cadere, veluti ab, ac, bc, etc., quatenus scilicet per divisionem infra N deprimuntur; at productum ex residuo in non-residuum in classe posteriore non-residuorum reperiri, ac denique producta ex binis non-residuis iterum fore residua. His notatis demonstrationem ita adornabimus, ut ostendamus, ingens absurdum esse secuturum, si nulla daretur formula $\lambda xx + \mu yy + \nu zz$ per numerum N divisibilis. Demonstratio autem sequenti modo procedet.

I. Quum omnia quadrata aequentur cuipiam residuo a, vel b, vel c, multiplo quodam numeri N aucto, si daretur talis formula $\lambda xx + \mu yy + \nu zz$ per numerum N divisibilis, ob $xx = \zeta N + a$, $yy = \eta N + b$ et $zz = \vartheta N + c$ foret utique formula $\lambda a + \mu b + \nu c$ per N divisibilis. Quare, qui nostrum theorema negaverit, statuere debet, nullam dari hujusmodi formulam $\lambda a + \mu b + \nu c$ per N divisibilem.

II. Quum igitur nulla detur hujusmodi formula per N divisibilis, multo minus fieri poterit $= 0$, ideoque ista aequatio: $\lambda a = -\mu b - \nu c$ erit impossibilis, pariter ac talis aequatio:

$$\lambda a = (\zeta N - \mu) b + (\eta N - \nu) c.$$

Verum quia λ, μ et ν sunt primi ad N, semper coefficientes ζ et η ita accipere licet, ut formulae $\zeta N - \mu$ et $\eta N - \nu$ fiant per λ divisibiles. Ponamus ergo $\zeta N - \mu = \lambda m$ et $\eta N - \nu = \lambda n$, atque impossibilis quoque erit ista aequatio: $a = mb + nc$.

III. Quum igitur ista formula $mb + nc$ non sit aequalis a, ideoque in classe residuorum non reperiatur (secundum mentem scilicet adversarii, qui nostrum theorema negat), necessario in altera classe non-residuorum reperietur; ibidem ergo etiam (quia c unitatem denotare potest) occurret $mb + n$, hincque adeo omnes istae formulae:

$$ma + n, \quad mb + n, \quad mc + n, \quad md + n, \text{ etc.},$$

quae cum omnes a se invicem diversae et numero sint $\frac{1}{2}(N - 1)$, his tota classis non-residuorum exhaurietur, quatenus scilicet divisae per N infra N deprimuntur.

IV. In eadem vero etiam classe occurrere debent omnia producta horum numerorum in quemlibet numerum primae classis veluti d ducta, quae ergo erunt

$$mad + nd, \quad mbd + nd, \quad mcd + nd, \text{ etc.}$$

Verum producta ad, bd, cd, in priorem classem cadunt, ac reperiuntur inter ipsos numeros a, b, c, d, etc., sicque in altera classe inter non-residua occurrent quoque omnes hae formulae:

$$ma + nd, \quad mb + nd, \quad mc + nd, \text{ etc.},$$

quae praecedentes singulas superant quantitate $n(d - 1)$. Hoc discrimen ponatur brevitatis gratia $= \omega$, quod utique ad ipsum divisorem N erit primum, si modo pro d non assumatur unitas, quia $d - 1$ est $< N$, atque etiam numerus n primus ad N.

V. Quodsi igitur in classe non-residuorum contineatur numerus α, ibidem quoque occurret $\alpha + \omega$, atque ob eandem rationem hic numerus, iterum incrementum ω accipiens, scilicet $\alpha + 2\omega$ ibi reperiatur necesse est; atque ob eandem rationem, etiam numeri $\alpha + 3\omega$, $\alpha + 4\omega$, etc. Omnes igitur termini hujus progressionis arithmeticae:

$$\alpha, \quad \alpha + \omega, \quad \alpha + 2\omega, \quad \alpha + 3\omega, \text{ etc.}$$

quatenus scilicet per N divisae infra N deprimuntur, inter non-residua occurrere debebunt.

VI. Quia differentia hujus progressionis est ω, numerus scilicet ad N primus, in hac progressione occurrunt termini non solum per N divisibiles, sed etiam insuper omnes, qui per N divisi pro residuis praebent omnes plane numeros 1, 2, 3, 4, etc. nullo excluso. Quocirca secundum mentem adversarii in classe non-residuorum omnes plane occurrerent numeri, 1, 2, 3, 4, etc. quod cum sit absurdum, opinio adversarii certe est falsa: scilicet falsum est, nullos dari numeros formae

$$\lambda xx + \mu yy + \nu zz,$$

qui sint per N divisibiles. Utique igitur tales numeri dabuntur; atque hoc ipsum est, quod praestare suscepimus.

Coroll. 1. Non solum autem semper tria hujusmodi quadrata xx, yy et zz reperire licet, sed etiam unum eorum, veluti zz, pro lubitu assumere licet, dum non sit per N divisibile. Ita si f

denotet numerum pro lubitu datum non divisibilem per N, semper assignare licebit bina quadrata xx et yy, ut formula $\lambda xx + \mu yy + \nu ff$ fiat per N divisibilis. Ad hoc demonstrandum, quicunque fuerit numerus z, semper dabitur ejusmodi numerus v, ut productum vz per N divisum relinquat datum residuum f. Sit enim $vz = \vartheta N + f$, et formula nostra per vv multiplicata, quae utique divisibilis erit per N, fiet

$$\lambda vvxx + \mu vvyy + \nu(\vartheta\vartheta NN + 2\vartheta Nf + ff)$$

ubi, quia membra $\vartheta\vartheta NN + 2\vartheta Nf$ per N sponte sunt divisibilia, etiam reliqua forma

$$\lambda vvxx + \mu vvyy + \nu ff$$

per N divisibilis erit.

Coroll. 2. Quicunque fuerint numeri λ, μ, ν, pro uno eorum semper unitatem aliumve numerum pro lubitu assumere licet. Quia enim, per ϑ multiplicando, haec formula:

$$\vartheta\lambda xx + \vartheta\mu yy + \vartheta\nu zz$$

divisionem per N admittit, loco ϑ ejusmodi numerum assumere licebit, ut productum $\vartheta\lambda$ per N divisum relinquat unitatem; tum autem haec formula:

$$xx + \vartheta\mu yy + \vartheta\nu zz$$

etiamnunc per N erit divisibilis. Quin etiam hic loco $\vartheta\mu$ et $\vartheta\nu$ residua ex divisione per N facta oriunda scribere licet, hocque modo formulam illi, quam Celeb. La Grange est contemplatus, omnino similem assequimur.

Scholion. Ecce ergo demonstrationem omnibus numeris absolutam tandem sumus assecuti theorematis illius notissimi, quod omnes plane numeri sint summae quatuor vel pauciorum quadratorum, quam quidem jam olim Fermatius se invenisse est professus, injuria autem temporum intercidisse etiamnunc maxime est dolendum. Nullum enim plane est dubium, quin Fermatii demonstratio multo simplicior et generalior fuerit, quam istae, quae nunc demum lucem aspexerunt. Quantum enim ex ejus monimentis suspicari licet, ex principiis longe diversis demonstrationem suam petiisse videtur: quandoquidem se asseverat ex eodem fonte demonstrasse, quod omnes plane numeri sint summae numerorum vel trium trigonalium vel pauciorum; tum etiam summae quinque pentagonalium aut pauciorum; nec non summae sex hexagonalium et ita porro; a qua generalitate nostra demonstratio longissime abest, atque etiamnunc demonstrationem ignoramus, quod omnis numerus sit summa trium vel pauciorum trigonalium. Interim tamen circa hoc theorema observari convenit, id tantum in numeris integris esse verum, dum alterum, quod hic demonstravimus etiam numeros fractos complectitur: omnes enim istae fractiones $\frac{1}{2}$, $\frac{3}{2}$, $\frac{5}{2}$, $\frac{7}{2}$, $\frac{9}{2}$, etc. nullo modo in ternos numeros trigonales resolvi se patiuntur, sive nullos valores rationales loco x, y, z invenire licet, ut fiat

$$\frac{1}{2} = \frac{xx+x}{2} + \frac{yy+y}{2} + \frac{zz+z}{2},$$

quare, quod maxime mirandum videtur, haec aequatio:

$$1 = xx + x + yy + y + zz + z$$

est impossibilis, quicunque etiam numeri fracti pro x, y, z accipiantur.

XXXIX.

Resolutio aequationis $Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$ per numeros tam rationales, quam integros.

(N. Comment. XVIII. 1773. p. 185. Exhib. 1772 Nov. 19.)

Haec forma latissime patens, quae insignem partem analyseos Diophanteae complectitur, pro varia indole numerorum A, B, C, D, E, F plures in se continet casus, qui vulgo diversis methodis tractari solent. Hic autem singulari modo ejus resolutionem sine radicis extractione ita docebo, ut solutio non solum ad numeros rationales, sed etiam integros accommodari possit.

1. In genere quidem resolutionem hujus aequationis tradere non licet, quia saepe usu venire potest, ut ea sit impossibilis, certissimum autem criterium possibilitatis solutionis sine dubio est, si unicus saltem casus, quo huic aequationi satisfiat, fuerit cognitus. Ponamus igitur hoc contingere casu, quo $x = a$ et $y = b$, ita ut revera sit:

$$Aa^2 + 2Bab + Cb^2 + 2Da + 2Eb + F = 0$$

et quemadmodum ex hoc casu cognito, alii sive numero finiti, sive infiniti, erui queant, hic sum ostensurus.

2. Subtrahatur ista aequatio ab ipsa proposita generali, ut obtineatur haec:

$$A(x^2 - a^2) + 2B(xy - ab) + C(y^2 - b^2) + 2D(x - a) + 2E(y - b) = 0,$$

cujus singula membra praeter secundum factorem habent vel $x - a$, vel $y - b$, at membrum secundum pluribus modis in duas partes resolvi potest, quarum altera habeat factorem $x - a$, altera $y - b$; est nempe: $xy - ab = x(y - b) + b(x - a) = y(x - a) + a(y - b)$; ut autem ambae litterae x et y parem rationem ineant, hac resolutione utamur:

$$2(xy - ab) = (x - a)(y + b) + (x + a)(y - b),$$

quo facto aequatio nostra sequentem induet formam

$$A(x-a)(x+a) + B(x-a)(y+b) + B(x+a)(y-b) + C(y-b)(y+b) + 2D(x-a) + 2E(y-b) = 0.$$

3. Consideretur nunc ratio quantitatum $x - a$ et $y - b$ tamquam data, ac statuatur

$$\frac{x-a}{y-b} = \frac{p}{q}, \quad \text{ita ut sit:} \quad qx - aq = py - bp,$$

qua ratione introducta nostra aequatio evadet:

$$Ap(x + a) + Bp(y + b) + Bq(x + a) + Cq(y + b) + 2Dp + 2Eq = 0,$$

ex quibus binis aequationibus utramque quantitatem quaesitam x et y definire licebit. Quum enim posterior sit

$$(x+a)(Ap+Bq)+(y+b)(Bp+Cq)+2Dp+2Eq=0,$$

prior vero praebeat:

$$y=\frac{qx-aq+bp}{p};$$

hic valor in illa substitutus dat:

$$(Ap^2+2Bpq+Cq^2)x+Aap^2+2Cbpq+2Bbp^2-Caq^2+2Dp^2+2Epq=0$$

unde colligitur

$$x=\frac{-a(Ap^2-Cq^2)-2b(Bp^2+Cpq)-2Dp^2-2Epq}{Ap^2+2Bpq+Cq^2}$$

hincque

$$y=\frac{+b(Ap^2-Cq^2)-2a(Bq^2+Apq)-2Dpq-2Eq^2}{Ap^2+2Bpq+Cq^2}.$$

4. Ecce ergo jam sumus assecuti solutionem generalissimam aequationis propositae in numeris rationalibus; quia enim ambos numeros p et q pro arbitrio assumere licet, evidens est, omnes plane solutiones in his formulis contineri debere. Quod autem solutiones in numeris integris attinet, manifestum est tales exhiberi non posse, nisi ambo numeratores illarum fractionum divisionem admittant per communem denominatorem $Ap^2+2Bpq+Cq^2$; id quod fieri nequit, nisi hic denominator ad numerum satis exiguum se reduci patiatur. Statim ergo hinc excludi oportet casus, quibus $B^2<AC$, sive quibus $AC-B^2$ est numerus positivus; tum enim quicunque valores loco p et q accipiantur, formulam $Ap^2+2Bpq+Cq^2$ non infra certum valorem deprimere licebit.

5. Quod si ergo numeri A, B et C ita fuerint comparati, ut per certos numeros p et q formula $Ap^2+2Bpq+Cq^2$ ad exiguum numerum, sive unitatem, sive binarium, tam positive quam negative sumtum redigi queat, omnes partes binarum formularum pro x et y inventarum abibunt in numeros integros. Posito autem isto numero $=\omega$, ita ut his casibus sit ω vel ± 1, vel ± 2, ob $Ap^2+2Bpq+Cq^2=\omega$, reperitur

$$p=\frac{-Bq\pm\sqrt{((BB-AC)q^2+A\omega)}}{A};$$

sic formula

$$(BB-AC)q^2+A\omega$$

debebit esse quadratum, quod quidem plerumque fieri poterit, quia pro ω sumi potest vel $+1$, vel -1, vel $+2$, vel -2, dummodo $BB-AC$ fuerit numerus positivus non quadratus, etiamsi sine dubio dantur casus, quibus ω majorem sortitur valorem. Tum vero habebitur:

$$x=\frac{a}{\omega}(Cq^2-Ap^2)-\frac{2b}{\omega}(Bp^2+Cpq)-\frac{2D}{\omega}p^2-\frac{2E}{\omega}pq,$$

$$y=\frac{b}{\omega}(Ap^2-Cq^2)-\frac{2a}{\omega}(Bq^2+Apq)-\frac{2D}{\omega}pq-\frac{2E}{\omega}q^2.$$

6. Utrum igitur nostra aequatio admittat solutiones in numeris integris, nec ne? judicium facillime instituitur; consideretur enim formula $BB-AC$, quae si fuerit numerus positivus non quadratus, semper adeo infinitis modis numerum q assignare licebit, ut formula illa radicalis abeat in numerum rationalem, indeque definietur alter numerus p, quibus adhibitis impetrabimus binos numeros satisfacientes x et y. Sufficiet autem pro q unicum valorem idoneum invenisse, dum ex

eo pro x et y successive innumerabiles valores satisfacientes deduci possunt, id quod operae pretium erit clarius ostendisse. Ponamus scilicet ex numeris primo satisfacientibus a et b hoc modo prodiisse sequentes:

$$x = \zeta a + \eta b + \vartheta \quad \text{et} \quad y = \lambda a + \mu b + \nu$$

atque si jam hi pro a et b adhibeantur, per easdem formulas novos deducemus valores pro x et y, qui denuo loco a et b assumti praebebunt iterum alios idoneos valores pro x et y, et ita porro.

7. Sint numeri, qui hoc modo successive pro x reperiuntur,

$$a,\ a',\ a'',\ a''',\ a^{\text{IV}},\ \text{etc.}$$

numeri autem pro y respondentes sint:

$$b,\ b',\ b'',\ b''',\ b^{\text{IV}},\ \text{etc.}$$

atque habebimus sequentes aequationes:

$$\begin{array}{ll} a' = \zeta a + \eta b + \vartheta, & b' = \lambda a + \mu b + \nu, \\ a'' = \zeta a' + \eta b' + \vartheta, & b'' = \lambda a' + \mu b' + \nu, \\ a''' = \zeta a'' + \eta b'' + \vartheta, & b''' = \lambda a'' + \mu b'' + \nu, \\ \text{etc.} & \text{etc.} \end{array}$$

Ex his relationibus eliminando litteras b, b', satis simplex relatio concluditur inter valores continuos a, a', a'', quae ita se habet:

$$a'' = (\mu + \zeta)\, a' + (\eta\lambda - \mu\zeta)\, a + \vartheta\,(1 - \mu) + \eta\nu.$$

Simili modo eliminando litteras a, a'

$$b'' = (\mu + \zeta)\, b' + (\eta\lambda - \zeta\mu)\, b + \lambda\vartheta + \nu\,(1 - \zeta),$$

unde patet utramque seriem esse recurrentem secundi ordinis, secundum eandem scalam relationis:

$$\zeta + \mu, \quad \eta\lambda - \zeta\mu$$

utrinque autem insuper numerum quendam absolutum addi oportet.

8. Cognita hac scala relationis formetur haec aequatio quadratica

$$z^2 = (\zeta + \mu)\, z + (\eta\lambda - \zeta\mu),$$

cujus binae radices sunt:

$$z = \tfrac{\zeta + \mu}{2} \pm \sqrt{\left(\left(\tfrac{\zeta - \mu}{2}\right)^2 + \eta\lambda\right)},$$

quarum potestatibus exprimi possunt termini generales utriusque seriei. Quo hoc clarius reddatur, sit prioris seriei

$$a,\ a',\ a'',\ a''',\ \text{etc.}$$

terminus quotuscunque $= x$, alterius vero seriei:

$$b,\ b',\ b'',\ b''',\ \text{etc.}$$

terminus generalis y, et posito brevitatis gratia

$$\tfrac{\zeta + \mu}{2} = r \quad \text{et} \quad \sqrt{\left(\left(\tfrac{\zeta - \mu}{2}\right)^2 + \eta\lambda\right)} = \sqrt{s},$$

pro priori serie statuatur

$$x = f\,(r + \sqrt{s})^n + g\,(r - \sqrt{s})^n + h,$$

eritque valor sequens

$$x' = f(r+\sqrt{s})(r+\sqrt{s})^n + g(r-\sqrt{s})(r-\sqrt{s})^n + h$$

huncque sequens

$$x'' = f(r+\sqrt{s})^2(r+\sqrt{s})^n + g(r-\sqrt{s})^2(r-\sqrt{s})^n + h.$$

Quare cum ex lege progressionis esse debeat;

$$x'' = (\zeta+\mu)x' + (\eta\lambda - \zeta\mu)x + \vartheta(1-\mu) + \eta\nu$$

si illi valores substituantur, potestates sponte se destruunt, ac resultat

$$h = \frac{\vartheta(1-\mu)+\eta\nu}{(1-\mu)(1-\zeta)-\eta\lambda}.$$

Pro coefficientibus autem f et g considerentur termini initiales ante definiti, et facto quidem $n=0$, prodeat $x=a$, hincque erit

$$a = f+g+h,$$

tum vero ponatur $n=1$, ut prodeat

$$x = a' = \zeta a + \eta b + \vartheta$$

fiatque ea

$$= f(r+\sqrt{s}) + g(r-\sqrt{s}) + h$$

et quia

$$f+g = a-h, \quad \text{erit} \quad a' = (a-h)r + (f-g)\sqrt{s} + h,$$

hincque

$$f-g = \frac{a'}{\sqrt{s}} - \frac{(a-h)r}{\sqrt{s}} - \frac{h}{\sqrt{s}} = \frac{a'-ar-h(1-r)}{\sqrt{s}}.$$

Eodem modo pro altera serie recurrente terminus generalis y reperietur, ita ut in genere nihil amplius desiderari possit.

9. Ceterum uti jam innuimus, dantur casus, quibus formula $App+2Bpq+Cqq$ neque ad unitatem, neque ad binarium deprimi potest; conveniet igitur litteras p et q ita assumi, ut huic formulae minimus valor concilietur, unde non parum egregium nascitur problema, quo datis numeris A, B, C quaeruntur valores litterarum p et q in integris, ut formula $App+2Bpq+Cqq$ minimum omnium accipiat valorem.

Alia resolutio ejusdem aequationis.

10. Quum tres termini initiales, per A multiplicati, factores habeant

$$(Ax+By+y\sqrt{(B^2-AC)}), \quad (Ax+By-y\sqrt{(B^2-AC)}),$$

totam aequationem sub tali forma repraesentare licebit:

$$(Ax+By+M+(y+N)\sqrt{(B^2-AC)})((Ax+By+M-(y+N)\sqrt{(B^2-AC)}) = O,$$

quae evoluta praebet

$$A^2x^2+2ABxy+ACy^2+2AMx+(2MB-2NB^2+2ACN)y+M^2-B^2N^2+ACN^2-O=0,$$

qua cum forma proposita comparata assequimur:

$$2AD = 2AM, \quad D = M,$$
$$2AE = 2MB - 2N(B^2-AC),$$
$$AF = M^2 - N^2(B^2-AC) - O,$$

hincque

$$M = D, \quad N = \frac{BD - AE}{B^2 - AC}, \quad O = D^2 - AF - \frac{(BD - AE)}{B^2 - AC}.$$

11. Inventis igitur valoribus M, N et O, ponatur brevitatis gratia $BB - AC = k$, ut aequatio nostra per factores irrationales expressa sit

$$(Ax + By + D + (y + N)\sqrt{k})(Ax + By + D - (y + N)\sqrt{k}) = O.$$

Et quia assumimus unam solutionem jam esse cognitam, qua sit $x = a$ et $y = b$, habebimus quoque

$$(Aa + Bb + D + (b + N)\sqrt{k})(Aa + Bb + D - (b + N)\sqrt{k}) = 0$$

quocirca bina haec producta inter se aequalia esse debebunt; statuamus hinc brevitatis gratia:

$$Ax + By + M = P, \quad y + N = Q,$$
$$Aa + By + M = G, \quad b + N = H,$$

ita ut nostra binorum productorum aequalitas fiat:

$$(P + Q\sqrt{k})(P - Q\sqrt{k}) = O = (G + H\sqrt{k})(G - H\sqrt{k}),$$

ubi notandum, si prior factor illius producti alterutri factori istius aequalis ponatur, tum quoque posteriorem factorem illius sponte alteri hujus aequalem esse futurum, quoniam discrimen tantum in signo quantitatis radicalis $\sqrt{k}$ est situm. Manifestum autem est, si factores priores inter se aequales statuantur, et partes tam rationales, quam irrationales seorsim aequentur, scilicet $P = G$ et $Q = H$, inde ipsum casum cognitum esse proditurum, nempe $x = a$ et $y = b$.

12. Sin autem hoc modo prior factor illius producti, posteriori hujus aequetur, ut sit

$$P + Q\sqrt{k} = G - H\sqrt{k},$$

nova solutio hinc elicietur; aequalitas enim

$$Q = -H \quad \text{dabit} \quad y + N = -b - N, \quad \text{sive} \quad y = -b - 2N,$$

unde altera conditio $P = G$ dabit

$$Ax - Bb - 2NB + M = Aa + Bb + M, \quad \text{seu}$$

$$Ax = Aa + 2Bb + 2NB, \quad \text{hincque} \quad x = a + \frac{2B(b + N)}{A}.$$

Ergo ex qualibet solutione jam inventa, puta $x = a$ et $y = b$, alia quasi sociata ex ea facillime concluditur; quippe quae si loco M et N valores assumti restituantur, praebebit

$$x = a + \frac{2B}{A}\left(b + \frac{BD - AE}{B^2 - AC}\right), \quad y = -b - \frac{2(BD - AE)}{B^2 - AC}.$$

Quae quidem solutio numeris fractis continetur, nisi forte numeratores fuerint per denominatores suos divisibiles.

13. Quo autem hinc plures atque adeo infinitas solutiones eliciamus, in subsidium vocemus formulam $s = \sqrt{(kr^2 + 1)}$, quippe quae methodo Pelliana semper infinitis modis resolvi potest, dummodo k non fuerit vel numerus negativus, vel numerus quadratus. Quum enim hinc fiat $s^2 - kr^2 = 1$, nostram aequationem hac forma repraesentare poterimus:

$$P^2 - kQ^2 = (G^2 - kH^2)(s^2 - kr^2).$$

Hincque per factores irrationales statuamus

$$P + Q\sqrt{k} = (G + H\sqrt{k})(s + r\sqrt{k}) = Gs + kHr + (Gr + Hs)\sqrt{k};$$

sic enim simul toti aequationi satisfiet, si quidem partes rationales et irrationales seorsim aequantur. At irrationales praebent:

$$Q = Gr + Hs, \quad y + N = Aar + Bbr + Mr + bs + Ns, \quad y = Aar + Bbr + Mr + bs + Ns - N.$$

At partes rationales dant:

$$P = Gs + kHr, \quad \text{seu} \quad Ax + By + D = Aas + Abs + Ds + kr + kNr,$$

unde

$$x = s\left(a + \frac{D - BN}{A}\right) + r\left(\frac{kb + kN - B^2 b - BD}{A} - Ba\right) + \frac{BN - D}{A}.$$

14. Nunc igitur loco litterarum M et N restituantur valores supra inventi, atque pro nostris quantitatibus quaesitis x et y sequentes reperiuntur formulae, si scilicet loco k scribatur $B^2 - AC$:

$$x = \left(a + \frac{EB - CD}{B^2 - AC}\right)s + (Ba + Cb + E)(-r) + \frac{CD - EB}{B^2 - AC},$$

$$y = \left(b + \frac{BD - AE}{B^2 - AC}\right)s + (Bb + Aa + D)r + \frac{AE - BD}{B^2 - AC},$$

ubi permutatio, quae inter litteras x et y locum habet, manifesto elucet.

15. Quod si hi valores pro x et y inventi loco a et b substituantur in istis formulis, pro x et y inde novi valores eruentur, qui denuo loco a et b sumti alios novos pro x et y praebebunt, et ita porro in infinitum. Verum omnes istos valores simul in formulis generalibus complecti licebit, uti jam supra fecimus. Sequenti autem modo idem negotium multo commodius et succinctius conficietur.

16. Quoniam $ss - krr = 1$, atque adeo omnes potestates ipsius $ss - krr$ etiam unitati aequantur, ponere poterimus

$$P^2 - kQ^2 = (G^2 - kH^2)(ss - krr)^n,$$

hincque per factores irrationales

$$P + Q\sqrt{k} = (G + H\sqrt{k})(s + r\sqrt{k})^n;$$

quia autem hujus potestatis aliae partes sunt rationales, aliae irrationales per $\sqrt{k}$ affectae, statuamus

$$(s + r\sqrt{k})^n = S + R\sqrt{k}$$

atque ut ante, hinc sequentes valores pro x et y eliciemus:

$$x = \left(a + \frac{EB - CD}{B^2 - AC}\right)S + (Ba + Cb + E)(-R) + \frac{CD - EB}{B^2 - AC},$$

$$y = \left(b + \frac{BD - AE}{B^2 - AC}\right)S + (Bb + Aa + D)R + \frac{AE - BD}{B^2 - AC}.$$

17. Quum autem sit

$$S + R\sqrt{k} = (s + r\sqrt{k})^n,$$

erit eodem modo

$$S - R\sqrt{k} = (s - r\sqrt{k})^n;$$

unde deducimus

$$S = \tfrac{1}{2}(s + r\sqrt{k})^n + \tfrac{1}{2}(s - r\sqrt{k})^n$$

et

$$R = \frac{1}{2\sqrt{k}}(s + r\sqrt{k})^n - \frac{1}{2\sqrt{k}}(s - r\sqrt{k})^n,$$

quibus valoribus substitutis, obtinebimus

$$x = \left(\frac{EB - CD}{2(B^2 - AC)} + \frac{a\sqrt{k} - Ba - Cb - E}{2\sqrt{k}}\right)(s + r\sqrt{k})^n$$
$$+ \left(\frac{EB - CD}{2(B^2 - AC)} + \frac{a\sqrt{k} + Ba + Cb + E}{2\sqrt{k}}\right)(s - r\sqrt{k})^n + \frac{CD - EB}{B^2 - AC},$$
$$y = \left(\frac{BD - AE}{2(B^2 - AC)} + \frac{b\sqrt{k} + Bb + Aa + D}{2\sqrt{k}}\right)(s + r\sqrt{k})^n$$
$$+ \left(\frac{BD - AE}{2(B^2 - AC)} + \frac{b\sqrt{k} - Bb - Aa - E}{2\sqrt{k}}\right)(s - r\sqrt{k})^n + \frac{AE - BD}{B^2 - AC},$$

et quia $k = B^2 - AC$, hae formulae ita simpliciores evadent:

$$x = \frac{1}{2k}\left(EB - CD + ak - (Ba + Cb + E)\sqrt{k}\right)(s + r\sqrt{k})^n$$
$$+ \frac{1}{2k}\left(EB - CD + ak + (Ba + Cb + E)\sqrt{k}\right)(s - r\sqrt{k})^n$$
$$+ \frac{1}{2k}\left(CD - EB\right),$$
$$y = \frac{1}{2k}\left(BD - AE + bk + (Bb + Aa + D)\sqrt{k}\right)(s + r\sqrt{k})^n$$
$$+ \frac{1}{2k}\left(BD - AE + bk - (Bb + Aa + D)\sqrt{k}\right)(s - r\sqrt{k})^n$$
$$+ \frac{1}{2k}\left(AE - BD\right).$$

18. Ante jam vidimus, quamlibet solutionem $x = a$ et $y = b$ suppeditare aliam sibi quasi sociam:

$$x = a + \frac{2B}{A}\left(b + \frac{BD - AE}{B^2 - AC}\right) \quad \text{et} \quad y = -b - \frac{2(BD - AE)}{B^2 - AC},$$

quia autem ex ipsa indole nostrae aequationis, litterae x et y inter se permutari possunt, dummodo

1) litterae a et b,
2) litterae A et C et
3) litterae D et E

inter se permutentur, haec consideratio nobis adhuc aliam solutionem suppeditabit, scilicet

$$x = -a - \frac{2(BE - CD)}{B^2 - AC}, \quad y = +b + \frac{2B}{C}\left(a + \frac{BE - CD}{B^2 - AC}\right).$$

Sicque ex eadem solutione duae novae sociae obtinentur.

19. Haec methodus posterior aequationem nostram resolvendi eo magis est notatu digna, quod ex doctrina irrationalium est petita, cujus alioquin nullus videtur esse usus in analysi Diophantea. Eximium autem hujus doctrinae usum jam pridem in algebra mea ruthenice et germanice edita fusius ostendi. Ceterum ad casus particulares nostrae aequationis propositae hic descendere non opus videtur, quum hujusmodi casus jam passim, satis superque sint pertractati.

XL.

De criteriis aequationis $fxx + gyy = hzz$, utrum ea resolutionem admittat, nec ne?

(Op. anal. I. 211 Exhib. 1772. Dec. 7.)

§ 1. Notum est hujusmodi aequationem, pro varia relatione, quae inter numeros f, g et h intercedit, modo esse possibilem modo impossibilem, siquidem pro x, y et z numeros rationales accipi oportet, atque adeo integros, quia fracti facillime ad integros revocarentur. Ita notum est hanc aequationem: $xx + yy = 2zz$ esse possibilem; hanc vero: $xx + yy = 3zz$ impossibilem. Quando autem litterae f, g et h majores tenent valores, judicium, utrum aequatio sit possibilis nec ne, difficulter instituitur; in maximis vero numeris vix suscipiendum videtur. Hic igitur constitui in certa criteria inquirere, ex quibus judicare liceat, utrum haec aequatio sit possibilis, nec ne, quantumvis magni fuerint numeri f, g et h.

§ 2. Ante omnia autem sequentia notasse juvabit:

I. Numeros f, g et h non solum integros assumo. sed etiam non-quadratos, neque etiam per quadratum divisibiles; si enim numerus f haberet factorem quadratum, is in quadrato xx involvi posset, quod etiam de reliquis tenendum.

II. Praeterea hos numeros aeque negativos ac positivos assumere licet; et quia aequatio ita semper disponi potest, ut membra fxx et hzz obtineant valores positivos, solum membrum gyy relinquitur, quod vel positivum vel negativum esse poterit.

III. Numeros f et g tamquam primos inter se spectamus: si enim haberent communem divisorem d, vel numerus h eundem habere deberet, quo casu ille per divisionem tolleretur; vel quantitas z per d esset divisibilis. Unde si loco z scribamus dv, nostra aequatio ad hanc formam reduceretur: $fxx + gyy = dhvv$, ita ut nunc f et g futuri sint primi inter se.

IV. Denique notandi sunt casus maxime obvii, quibus aequatio nostra fit possibilis. Primo scilicet hoc evenit, si fuerit vel $h = f$, vel $h = g$: illo enim casu foret $y = 0$ et $z = x$, hoc vero $x = 0$ et $z = y$. Tum vero etiam casus satis obvius erit, si fuerit $h = f + g$, quia ei satisfieret, sumendo $z = x = y$. Minus obvii autem erunt casus, quibus $h = faa + gbb$; foret enim tum $x = a$, $y = b$ et $z = 1$.

§ 3. Primum autem investigabo, datis numeris f et g, cujusmodi numeri pro h locum habere queant, ut aequatio fiat possibilis. Quare cum hic b ut numerum incognitum spectemus, aequationem nostram hac forma referamus: $fxx + gyy = hzz$, ut jam idoneos valores pro littera s investigari oporteat, quibus aequatio fiat possibilis, et quidem omnes qui hoc praestent; quem in finem sequentia theoremata adjungo.

§ 4. **Theorema 1.** Si casu $s=h$ possibilis fuerit aequatio $fxx+gyy=hzz$, ita ut litterae x, y, z jam sint cognitae, si vero insuper habeatur haec aequatio:

$$pp+fgqq=krr,$$

tum nostra aequatio quoque erit possibilis casu $s=hk$.

Demonstratio. Multiplicentur enim hae duae aequationes in se, et prodibit haec nova aequatio

$$hkrrzz=(fxx+gyy)(pp+fgqq)=f(px\pm gqy)^2+g(py\mp fqx)^2.$$

Quare si statuamus

$$rz=Z,\quad px\pm gqy=X \quad\text{et}\quad py\mp fqx=Y,$$

nascitur haec aequatio propositae omnino similis:

$$fX^2+gY^2=hkZ^2.$$

§ 5. **Coroll. 1.** Quodsi ergo litterae p et q ita assumere liceat, ut k obtineat factorem h, scilicet $k=hl$, tum ob $s=hhl$ novus valor idoneus erit $s=l$, quoniam quadratum hh omittere licet.

§ 6. **Coroll. 2.** Quemadmodum igitur ex illo valore idoneo $s=h$ erutus est alius $s=hk$, sive $s=l$, ita ex hoc simili modo alius novus valor, puta $s=m$, hincque denuo novus $s=n$ erui poterit; atque hanc determinationem in infinitum continuare licebit. Ita ex casu quocunque cognito innumerabiles alii derivari poterunt.

§ 7. **Coroll. 3.** Si eveniat ut numeri h et k communem habeant divisorem d, tum novus valor fk factorem habebit dd, qui ergo expungi poterit. Hoc modo continuo ad minores numeros idoneos pro s pervenire licebit, donec tandem ad casum obvium perducamur.

§ 8. **Coroll. 4.** Hinc si adhuc fuerimus incerti, utrum h sit valor idoneus ipsius s, hoc autem modo procedendo perveniamus tandem ad casum obvium, tuto concludere poterimus, etiam casum $h=k$ esse possibilem. Sin autem hoc nullo modo succedat, vel tandem in minoribus numeris ad ejusmodi casum perveniatur, cujus impossibilitas patescat, etiam valor ipse $h=k$ pro impossibili erit habendus.

§ 9. **Theorema 2.** Si pro nostra aequatione tres innotescant casus possibiles $s=h$, $s=h'$ et $s=h''$, tum etiam valor idoneus erit $s=h.h'.h''$.

Demonstratio. Quum igitur habeantur tres hujusmodi aequationes, quae sint:

$$\begin{aligned} &\text{I.} && faa+gbb=h.cc,\\ &\text{II.} && fAA+gBB=h'.CC,\\ &\text{III.} && f\alpha\alpha+g\beta\beta=h''.\gamma\gamma, \end{aligned}$$

ducatur prima in secundam, et productum erit

$$hh'.ccCC=(faa+gbb)(fAA+gBB)=(faA\pm gbB)^2+fg(aB\mp bA)^2.$$

Faciamus nunc

$$cC=r\quad\text{et}\quad faA\pm gbB=p\quad\text{et}\quad aB\mp bA=q,$$

ut hoc productum fiat

$$pp+fgqq=hh'rr,$$

quod denuo multiplicatum in tertiam aequationem dabit tale productum:

$$hh'h''rr\gamma\gamma = (f\alpha\alpha + g\beta\beta)(pp + fgqq) = f(p\alpha \pm gq\beta)^2 + g(p\beta \mp fq\alpha)^2,$$

quae forma cum plane conveniat cum proposita, veritas theorematis est manifesta, et casus $s = hh'h''$ erit possibilis.

§ 10. **Coroll. 1.** Ex cognitis ergo tribus valoribus idoneis h, h', h'', quartus facile invenitur. Ac si forte illi terni habeant divisores communes, hoc modo ad novos valores continuo minores pertingere licebit.

§ 11. **Coroll. 2.** Si ergo hunc novum valorem indicemus littera h''', tum etiam valores idonei erunt $s = hh'h'''$, $s = hh''h'''$, $s = h'h''h'''$; ex quibus porro simili modo plures alii deduci possunt.

§ 12 **Coroll. 3.** Quando autem hi novi valores per quadrata, uti praecepimus, deprimuntur, continuo iidem casus cogniti recurrent. Quum enim sit $h''' = hh'h''$, forma $hh'h'''$ reducitur ad h'', haec vero: $hh''h'''$ ad h', et $h'h''h'''$ ad h, ita ut revera unus tantum casus novus hoc modo reperiatur.

§ 13. **Theorema 3.** Si aequationi nostrae $fxx + gyy = szz$ satisfaciat casus $s = h$, tum quoque omnes isti valores satisfacient:

$$s = 4fg + h, \quad s = 8fg + h, \quad s = 12fg + h, \quad s = 16fg + h, \text{ etc.}$$

quin etiam, si h fuerit numerus satis magnus, isti:

$$s = h - 4fg, \quad s = h - 8fg, \quad s = h - 12fg,$$

et in genere $s = h \pm 4nfg$, dummodo hi numeri fuerint primi.

Hujus elegantissimi theorematis demonstratio adhuc desideratur, postquam a pluribus jam dudum frustra est investigata; cujus rei difficultas manifesto in hoc est sita, quod omnes hi numeri tum demum quaesito satisfaciant, quando sunt numeri primi. Quando enim sunt compositi, evenire potest, ut non satisfaciant, etiamsi non semper a scopo aberrent. Quum autem hic tantum valeant numeri primi, probe notandum est, numeros negativos, qui ex formula $s = h - 4fg$ resultare possunt, non pro primis esse habendos. Quocirca plurimum is praestitisse erit censendus, cui successerit demonstrationem hujus theorematis invenire.

§ 14. **Coroll. 1.** Quum hoc modo saltem ascendendo in infinitum progredi liceat, etiam multitudo valorum idoneorum pro s eo usque augeri poterit, quousque tabula numerorum primorum fuerit constructa.

§ 15. **Coroll. 2.** Ita quum haec aequatio: $xx + yy = zz$ sit possibilis, ubi est $f = 1$, $g = 1$ et $s = h = 1$, haec forma: $4n + 1$, quatenus scilicet praebet numeros primos, etiam totidem valores idoneos pro s suppeditabit, qui numeri sunt

1, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc.

Hos autem numeros omnes ipsos aequari summae duorum quadratorum, jam dudum rigorosissime a me est demonstratum, unde eo minus de demonstratione reliquorum casuum desperare fas est. His igitur omnibus casibus licebit sumere $z = 1$. Interim tamen hinc etiam numeros compositos pro s invenire licet, dum per theorema primum producta ex binis vel pluribus horum ipsorum numerorum etiam pro s valebunt, quoniam binae illae formulae $fxx + gyy$ et $pp + fgqq$ hoc casu congruunt.

§ 16. **Coroll. 8.** Quia aequationi $2xx + 3yy = szz$ satisfieri potest casu $s = 341$, alios casus idem praestantes dabit formula $341 \pm 24n$, quoties scilicet prodierint numeri primi. Hinc ergo descendendo oriuntur sequentes valores:

$$341,\ 317,\ 293,\ 269,\ 197,\ 173,\ 149,\ 101,\ 53,\ 29,\ 5.$$

Hi autem omnes numeri ipsi jam in forma $2xx + 3yy$ continentur, ita ut possit esse $z = 1$.

§ 17. **Scholion.** Hoc theoremate, quasi demonstratum esset, praemisso, pro quovis casu numerorum f et g omnes plane valores idonei litterae s facile inveniri poterunt. Ad hoc autem ostendendum, duos casus separatim tractari oportet: priorem, quo $f = 1$, atque idcirco primi termini primi theorematis inter se conveniunt, alterum vero, quo f non est unitas. Unde primo aequationem $xx + gyy = szz$ evolvemus.

§ 18. **Problema 1.** Proposita aequatione $xx + gyy = szz$, invenire omnes valores idoneos pro s, quibus haec aequatio evadit possibilis.

Solutio. Hic statim evidens est valorem idoneum fore $s = g$; tum enim fit $x = 0$ et $y = z$. Etsi enim $4g$, $9g$, $16g$, etc. aeque satisfaciant, tamen omnes per quadratum depressi redeunt ad g. Verum sumto $y = 0$, omnes numeri quadrati pro s prodeunt, quos igitur omnes ad unitatem reducere liceret. Sed quia praeter hos ipsos numeros etiam iidem, numeris $4ng$ sive aucti; sive minuti satisfaciunt, quatenus scilicet prodeunt numeri primi, haec quadrata hic negligere non licet. Iis autem tantum quadratis indigemus, quae ad numerum $4g$ fuerint primi, quia aliter nulli numeri primi inde emergerent; quamobrem statim omnia quadrata paria hinc excluduntur, et iis tantum imparibus locus conceditur, quorum radices ad numerum g fuerint primi. Semper ergo hic occurrit unitas, tum vero etiam 9, nisi g sit per 3 divisibilis, porro etiam 25, nisi g divisorem habeat 5, etc. Quando autem haec quadrata excedunt numerum $4g$, eorum loco scribantur residua ex divisione per $4g$ remanentia. Ponamus ergo hinc prodire formulas:

$$4ng + 1,\quad 4ng + a,\quad 4ng + b,\quad 4ng + c,\quad 4ng + d,\quad \text{etc.},$$

ubi scilicet a, b, c, d, sunt ea residua, quae ex quadratis per $4g$ divisis resultant. Verum praeter hos casus, alius est obvius $s = 1 + g$, siquidem g fuerit numerus par; sin autem fuerit impar, sumatur $s = 4 + g$, ut scilicet habeatur numerus ad $4g$ primus. Tum vero quia per theorema primum producta ex binis numeris satisfacientibus etiam satisfaciunt, habebimus insuper istas formulas, loco $1 + g$, vel $4 + g$ scribendo h:

$$s = 4ng + h,\quad 4ng + ah,\quad 4ng + bh,\quad 4ng + ch,\quad 4ng + dh,\quad \text{etc.},$$

quos omnes valores conjunctim ita ob oculos constituamus:

$$s = 4ng + \begin{Bmatrix} 1, & a, & b, & c, & d, & \text{etc.} \\ h, & ah, & bh, & ch, & dh, & \text{etc.} \end{Bmatrix}$$

Quae omnes formulae eatenus valent, quatenus numeros primos producunt, hocque modo omnes plane numeri primi idonei reperientur; compositi autem nulla plane laborant difficultate, quum nascantur ex duobus pluribusve numeris primis idoneis. Quin etiam ipsum numerum g, ejusque producta per numeros jam inventos, annumerari oportet.

§ 19. **Coroll. 1.** Quia veritas hujus solutionis nondum plane est evicta, casus aliquos obvios consideremus, quos semper in aliqua superiorum formularum contineri deprehendemus. Ita casus $s = 1 + 4g$ continetur in formula $4ng + 1$, et $s = 1 + 9g$ continetur in formula $4ng + h$, si fuerit $h = 1 + g$; at si $h = 4 + g$, in ea continebitur $s = 4 + 9g$. Similique modo res se habet in formulis $1 + 16g$, $1 + 25g$, $1 + 36g$, etc., vel $4 + g$, $4 + 9g$, $4 + 25g$, etc., ubi eos casus, qui numeros primos producere nequeunt, excludimus.

§ 20. **Coroll. 2.** Haec solutio aeque locum habet, sive g sit numerus positivus, sive negativus. At quia hoc posteriori casu, in formulis inventis littera h obtinet valorem negativum, loco terminorum h, ah, bh, ch, etc., eorum complementa ad numerum $4g$ scribantur.

§ 21. **Coroll. 3.** Casu quo g est numerus negativus, si jam fuerint inventae formulae superiores, quae valent pro formula $xx - gyy$, si ibi signa mutentur, sive loco numerorum 1, a, b, c, d, etc. scribantur eorum complementa ad $4g$, tum illae inservient huic aequationi:

$$gyy - xx = szz.$$

§ 22. **Scholion.** Haec autem maxime illustrabuntur et facilius in usum vocari poterunt, si plura exempla adjungamus, quibus etiam natura numerorum aliaeque abstrusae proprietates clarius perspicientur.

§ 23. **Exempl. 1.** Sit $g = 1$ et aequatio proposita $xx + yy = szz$, atque hic pro valoribus ipsius s unica habetur formula $4n + 1$. Casus autem $1 + g = 2$, quia ad $4g$ non est primus, generali formulae innecti nequit; interim tamen seorsim praebet numerum idoneum $= 2$. Pro numeris igitur primis satisfacientibus praeter 2 habemus superiorem seriem:

$$1,\ 5,\ 13,\ 17,\ 29,\ 37,\ 41,\ \text{etc.}$$

et producta ex quocunque horum praebebunt omnes numeros compositos satisfacientes. At pro casu $g = -1$, seu aequatione $xx - yy = szz$, praeter formam $4n + 1$, ex quadratis ortam, formula $4 + g = 3$ dabit insuper hanc: $4n + 3$. Sicque omnes numeri primi in alterutra harum duarum formularum: $4n + 1$ et $4n + 3$ erunt contenti, ideoque omnes plane numeri primi hoc casu sunt idonei, quippe quos omnes in differentiam duorum quadratorum resolvere licet. Hinc quidem 2 excluditur, quoniam differentia duorum quadratorum esse nequit, attamen valorem pro s dari potest, siquidem pro z sumatur numerus par. Nam $2 . 4$ utique est $9 - 1$.

§ 24. **Exempl. 2.** Sit nunc $g = 2$ et proposita haec forma: $xx + 2yy = szz$, ubi quum sit $4g = 8$, quadrata imparia 1, 9, 25, etc. omnia reducuntur ad eandem formam $8n + 1$; at casus $1 + g = h = 3$ insuper dat hanc formam: $8n + 3$, sicque omnes numeri primi hac specie referentur: $8n \pm (1,\ 3)$, quibus accedit insuper $s = g = 2$, sicque omnes hi numeri primi sunt

$$1,\ 3,\ 11,\ 17,\ 19,\ 41,\ 43,\ 59,\ 67,\ 73,\ 83,\ 89,\ 97,\ \text{etc.}$$

At si sit $g = -2$, pro formula $xx - 2yy = szz$ reperitur $s = 8n + (1,\ 7)$, quibus annumerari debet -2, atque hinc vicissim pro aequatione $2yy - xx = szz$, erit $s = 8n + (7,\ 1)$. Iidem ergo numeri pro his duobus posterioribus casibus valent.

§ 25. **Exempl. 3.** Pro formula $xx + 3yy = szz$ secundum praecepta data prodit

$$s = 12n + (1,\ 7),$$

et insuper numerus solitarius 3. Pro formula autem $xx - 3yy = szz$ reperitur $s = 12n + (1)$.

§ 26. **Exempl. 4.** Pro formula $xx + 5yy = szz$ reperitur $s = 20n + (1, 9)$, cum numero 5; at pro formula $xx - 5yy = szz$ reperitur $s = 20n + (1, 9)$, cum numero -5.

§ 27. **Exempl. 5.** Pro formula $xx + 6yy = szz$ reperitur $s = 24n + (1, 7)$, una cum numero 6; pro formula autem $xx - 6yy = szz$ colligitur $s = 24n + (1, 19)$, una cum numero -6, ubi numeri ± 6 tamquam primi sunt spectandi, etiamsi in se sint compositi.

§ 28. **Scholion.** Plura hujusmodi exempla non evolvimus, quum calculus satis sit perspicuus, sed potius tabulam sequentem adjungimus, in qua pro quavis formula $xx + gyy = szz$, primo formam numerorum primorum pro s exhibebimus, deinde vero ipsos numeros primos usque ad centum; quibus cognitis omnia producta, tam ex binis quam pluribus numeris primis, pro valore litterae s satisfaciunt:

$xx + yy = szz$	$s = 4n + 1$ cum 2
numeri primi	1, 2, 5, 13, 17, 29, 37, 41, etc.
$xx - yy = szz$	$s = 4n + (1, 3)$
numeri primi	1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, etc.
$xx + 2yy = szz$	$s = 8n + (1, 3)$ cum 2
numeri primi	2; 1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97
$xx - 2yy = szz$	$s = 8n + (1, 7)$ cum -2
numeri primi	-2; 1, 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97
$xx + 3yy = szz$	$s = 12n + (1, 7)$ cum 3
numeri primi	3; 1, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
$xx - 3yy = szz$	$s = 12n + 1$ cum solitario -5
numeri primi	-5; 1, 13, 37, 61, 73, 97
$xx + 5yy = szz$	$s = 20n + (1, 9)$ cum numero 5
numeri primi	5; 1, 29, 41, 61, 89
$xx - 5yy = szz$	$s = 20 + (1, 9, 11, 19)$ cum numero -5
numeri primi	-5; 1, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89
$xx + 6yy = szz$	$s = 24n + (1, 7)$ cum numero 6
numeri primi	6; 1, 7, 31, 73, 79, 97
$xx - 6yy = szz$	$s = 24n + (1, 19)$ cum -6
numeri primi	-6; 1, 19, 43, 67, 73, 97
$xx + 7yy = szz$	$s = 28n + (1, 11, 23, 9, 25, 15)$ cum numero 7
numeri primi	7; 1, 11, 23, 29, 37, 43, 53, 67, 71, 79
$xx - 7yy = szz$	$s = 28n + (1, 9, 25)$ cum -7
numeri primi	-7; 1, 29, 37, 43, 83

$xx + 10yy = szz$	$s = 40n + (1, 9, 11, 19)$ cum 10
numeri primi	10; 1, 11, 19, 41, 59, 89
$xx - 10yy = szz$	$s = 40n + (1, 9, 31, 39)$ cum -10
numeri primi	-10; 1, 31, 41, 71, 79, 89
$xx + 11yy = szz$	$s = 44n + (1, 9, 25, 5, 37, 15, 3, 23, 31, 27)$ cum 11
numeri primi	$+11$; 1, 3, 5, 23, 31, 37, 47, 53, 59, 67, 71, 89, 97
$xx - 11yy = szz$	$s = 44n + (1, 9, 25, 5, 37)$ cum -11
numeri primi	-11; 1, 5, 37, 53, 89, 97.

§ 29. **Problema 2.** Proposita aequatione $fxx + gyy = szz$, invenire omnes numeros primos, qui pro s valores idoneos praebent, quibus haec aequatio evadit possibilis.

Solutio. Sit h valor quicunque idoneus pro s, et per theorema nondum demonstratum patet, omnes numeros primos in hac formula contentos: $4nfg + h$, pariter pro s valere; ex quo manifestum est, istum valorem h ad $4fg$ primum esse debere. Talis autem valor facile invenitur. Si enim ambo numeri f et g fuerint impares, capi poterit $h = 4f + g$, sive $h = f + 4g$; sin autem numerorum f et g alter fuerit par, alter impar, valor idoneus habetur $h = f + g$. Quo autem alii insuper numeri primi, atque adeo omnes, pro s obtineantur, consideretur formula $pp + fgqq = krr$, atque in problemate praecedente jam assignavimus omnes primos pro k valentes, qui sint

$$4nfg + (1,\ a,\ b.\ c,\ d,\ \text{etc.});$$

nunc hae duae aequationes ducantur in se, et jam ostendimus prodire hujusmodi formam: $hkrrzz$, sive $hkZ^2 = fX^2 + gY^2$, quocirca productum hk etiam dabit valorem idoneum pro s: unde perspicuum est, omnes numeros primos pro s idoneos contineri debere in hac forma generali:

$$s = 4nfk + (h,\ ah,\ bh,\ ch,\ dh,\ \text{etc.}).$$

Cognitis autem numeris primis pro s valentibus, qui nostrae aequationi $fxx + gyy = szz$ satisfaciunt, si insuper omnes numeri primi pro k adhibendi innotescant, qui sint A, B, C, D, etc., tum producta priorum pro s inventorum in singulos, vel binos, vel ternos etc. horum posteriorum praebebunt etiam valores idoneos pro s, hocque adeo modo facile erit infinitos valores litterae x exhibere.

§ 30. **Coroll. 1.** Si eveniat ut primus valor pro h inventus sit quadratus, tum, quia is jam in ordine numerorum 1, a, b, c, d, etc. continetur, iidem valores pro s locum habebunt, qui pro k sunt assignati.

§ 31. **Coroll. 2.** Sin autem numerus h in ordine 1, a, b, c, d non contineatur, tum nullo modo fieri poterit, ut valores pro s et k inter se conveniant, sed omnes a se invicem discrepabunt.

§ 32. **Exempl. 1.** Proposita sit aequatio $2xx + 3yy = szz$, ubi $f = 2$ et $g = 3$, primus autem valor $h = 5$. Tum ergo consideretur aequatio $pp + 6qq = krr$, et vidimus valores primos pro k contineri in hac formula: $24n + (1, 7)$. His igitur numeris 1, 7 in $h = 5$ ductis, omnes numeri primi pro s in hac formula continentur: $24n + (5, 11)$, qui sunt: 5, 11, 29, 53, 59, 83, etc.

Pro aequatione $2xx - 3yy = szz$, ubi $f = 2$ et $g = -3$, valor cognitus habetur $h = -1$, sive $h = 23$; at aequationi $pp - 6qq = krr$, pro k inventa est formula $24n + (1, 19)$, unde omnes numeri primi pro s fiunt: $24n + (5, 23)$, quae formula praebet hos numeros primos:

$$5,\ 23,\ 29,\ 47,\ 53,\ 71,\ \text{etc.}$$

Verum pro hac aequatione $3xx - 2yy = szz$, ubi $f = 3$ et $g = -2$, valor h fit $= 1$; et quia formula $pp - 6qq = krr$ eadem est quae ante, iidem etiam numeri primi pro s in formula $24n + (1, 19)$ continentur, hincque ipsi numeri primi: $24n + (5, 23)$, qui igitur fient:

$$5,\ 23,\ 29,\ 47,\ 53,\ 71,\ \text{etc.}$$

§ 33. **Exempl. 2.** Proposita aequatione $2xx + 5yy = szz$, ubi $f = 2$ et $g = 5$, primus valor h fit $= 7$, et quia aequationi $pp + 10qq = krr$ convenit formula

$$40n + (1,\ 9,\ 11,\ 19),$$

pro valoribus primis ipsius s habebimus

$$s = 40n + (7,\ 23,\ 37,\ 13),$$

ergo ipsi numeri primi erunt

$$7,\ 13,\ 23,\ 37,\ 47,\ 53,\ \text{etc.}$$

At proposita aequatione $2xx - 5yy = szz$, fit statim $h = -3$; et quia pro aequatione $pp - 10qq = krr$ invenimus formulam $40n + (1, 9, 31, 39)$, numeri primi quaesiti continebuntur in hac formula:

$$40n + (37,\ 13,\ 27,\ 3);$$

ergo ipsi numeri primi erunt:

$$3,\ 13,\ 37,\ 43,\ 53,\ 67,\ 83,\ \text{etc.}$$

Denique pro formula $5xx - 2yy = szz$, ob $h = 3$, ex iisdem numeris k numeri quaesiti pro s sunt:

$$40n + (37,\ 13,\ 27,\ 3).$$

§ 34. **Scholion 1.** Quae hactenus jam tradita hisque exemplis illustrata sunt, omnes numeros primos pro s satisfacientes suppeditant, qui in se invicem multiplicati, uti praecepimus, dant numeros compositos aeque satisfacientes. Neque vero hinc semper omnes plane numeri compositi pro s idonei obtinentur; sed dantur casus, quibus praeterea alii numeri primi in valores compositos ipsius s ingrediuntur. Causa hujus rei in eo consistit, quod in investigatione superiori numeros pares statim exclusimus, qui tamen, cum aliis numeris primis juncti, quaesito satisfacere possunt. Ad hos ergo eruendos ponamus statim $s = 2h$, ut sit

$$\frac{fxx + gyy}{2} = hzz.$$

Quod si jam haec formula $\frac{fxx + gyy}{2}$ praebeat numerum imparem, sive productum ex impari in quadratum par, ex eo statim infinitos alios valores pro h elicere licet. Sit enim α ejusmodi numerus impar, et quum pro forma $xx + fgyy = szz$ omnes valores primi ipsius s in hac forma contineantur: $4fg + (1, a, b, c, d, \text{etc.})$, omnes numeri primi idonei pro nostra littera h in hac forma continebuntur:

$$4fg + (\alpha,\ \alpha a,\ \alpha b,\ \alpha c,\ \alpha d,\ \text{etc.}),$$

qui si fuerint diversi ab iis, quos ante sumus assecuti, etiam infiniti alii habebuntur numeri primi, qui in compositionem numeri s ingredi possunt. Singuli enim isti numeri, quos litteris A, B, C, D designemus, per 2 multiplicati, idoneos praebent valores pro s, qui ergo erunt: $2a$, $2b$, $2c$, $2d$, etc. Et quia producta ex binis eorum etiam satisfaciunt, hinc nascentur numeri impares,

$$ab, \; ac, \; ad, \; bc, \; bd, \; cd, \; \text{etc.}$$

Ita in exemplo $xx - 3yy = szz$, formula $\frac{xx - 3yy}{2}$ statim dat -1. Quum ergo pro hoc casu inventa sit formula $s = 12n + 1$, pro valoribus ipsius h habebimus formulam $12n - 1$, sive $12n + 11$, quae praebet hos numeros primos: 11, 23, 47, 59, 71, 83, qui duplicati omnes etiam satisfaciunt, atque etiam producta ex eorum binis, tum vero etiam producta ex his in singulos eorum, quos ante jam assignavimus; hocque pacto multitudo valorum compositorum vehementer augetur. Hoc praecipue iis casibus usu venit, ubi formulae supra inventae ex paucioribus membris constabant. Pro formula autem $xx + 7yy = szz$, ejus dimidium $\frac{xx + 7yy}{2}$ praebet 4, sive $1 = a$, qui valor quum jam in formula supra data contineatur, hinc novi valores non oriuntur. At vero formula $\frac{xx - 7yy}{2}$ praebet $a = -3$, ideoque valores pro h erunt $28n + (25, 1, 9)$, qui numeri jam antea occurrunt. Hoc ergo probe observare oportet eum, qui etiam omnes numeros compositos pro s satisfacientes investigare voluerit, unde huic negotio immorari superfluum foret.

§ 35. **Scholion 2.** Quantumvis autem haec egregia videantur, utique hic erit dolendum, quod nondum firmis demonstrationibus sunt munita, cujus rei ratio potissimum in eo sita videtur, quod formulae pro s inventae eatenus tantum valent, quatenus numeros primos suppeditant. Quamquam autem omnes labores a me suscepti spem meam fefellerunt, tamen spero, conatus meos iis, qui hujusmodi speculationibus delectantur, non fore ingratos, praecipue quia jam memoratam illam difficultatem circa numeros primos de medio sustuli, ita ut nunc sine dubio aditus ad ista numerorum mysteria non mediocriter facilior reddi videatur.

§ 36. **Propositio 1.** Si fuerit $fxx + gyy = szz$, existente s numero primo, tum si omnia quadrata per hunc numerum s dividantur et residua ex singulis enata notentur, inter ea semper occurret $-fg$, sive sublata negatione, $s - fg$.

Demonstratio. Sint residua illa ex divisione per s orta, 1, a, b, c, d, etc., ac praebeat quadratum xx residuum a, quadratum vero yy residuum b, atque evidens est numerum $fa + gb$ per s fore divisibilem. Sit ergo $fa + gb = \lambda s$, eritque $gb = \lambda s - fa$, ideoque $bgg = \lambda gs - fga$. Quum jam omne residuum, in quadratum ductum, iterum inter residua occurrat, siquidem infra s deprimatur, prodeat inde residuum c, ita ut sit $c = \lambda gs - fga$, et multiplo ipsius s sublato $c = -fga$, sive $c = s - fga$, et quia hoc aeque valet de omnibus residuis, loco a sumentes unitatem habebimus: $c = -fg$, sive $c = s - fg$.

§ 37. **Coroll. 1.** Si ergo satisfaciat valor $s = h$, quia formula $4nfg + h$, si fuerit numerus primus, etiam satisfaciat pro s, si per hunc numerum omnia quadrata dividantur, inter residua certo occurret $-fg$.

§ 38. **Coroll. 2.** Sit ille divisor $=D$, et quia datur quadratum, quod sit pp, unde nascitur residuum $-fg$, manifestum est formulam $pp+fg$ divisibilem fore per divisorem D.

§ 39. **Coroll. 3.** Hic autem jam manifesto involvitur difficilis illa conditio numeri primi, quia ordo residuorum hic memoratus locum non habet, nisi D sit numerus primus. Fieri enim utique posset, ut $-fg$ non inter residua occurreret, si divisor non esset primus.

§ 40. **Propositio 2.** Si quadrata dividendo per quemcunque numerum primum $D=2P+1$ inter residua occurrat numerus r, tunc ejus potestas r^P per D divisa unitatem relinquet; et vicissim, si r^P-1 divisorem habeat D, numerum r inter residua reperiri necesse est.

Demonstratio. Quum divisor D ponatur $2P+1$, omnium numerorum ipso minorum multitudo est $2P$, quorum quia semissis tantum in residua ingreditur, multitudo residuorum erit P. Deinde etiam certum est, si inter residua occurrat numerus r, tum quoque omnes ejus potestates ibidem occurrere debere, quemadmodum simplicissima $r^0=1$ inest. Quocirca potestas r^P necessario non novum residuum praebere potest. Atque hinc rite concluditur, inde ipsum primum residuum 1 prodire debere, sicque constat propositam potestatem r^P, per numerum primum D divisam, residuum relinquere $=1$. Quod ad inversionem propositionis attinet, perpendamus, formulam $r^{2P}-1$ perpetuo divisibilem esse per $2P+1$; ex quo sequitur, vel formulam $r^{2P}-1$, vel r^P+1 divisibilem esse debere. Omnes ergo numeri pro r sumti, quibus formula posterior r^P+1 fit divisibilis, ex ordine residuorum excluduntur, atque illi tantum, qui formulam r^P-1 divisibilem producunt, relinquuntur, quorum numerus quum sit P, sequitur omnes numeros r fore residua.

§ 41. **Coroll. 1.** Quum primus divisor fuerit $=h$, ponamus $h=2p+1$, et quia $r=-fg$, sequitur, formulam $(-fg)^p-1$ per $h=2p+1$ esse divisibilem, seu fore $r^p=1+m(2p+1)$. Quum deinde etiam divisor esse possit $h+4nfg$, dummodo fuerit numerus primus, ob $h=2p+1$ faciamus

$$D=2p+1+4nfg=2P+1,$$

ita ut sit $P=p+2nfg$, atque etiam haec potestas:

$$(-fg)^P=(-fg)^{p+2nfg}$$

unitate minuta per divisorem $2p+1+4nfg$ evadet divisibilis.

§ 42. **Coroll. 2.** Quocirca totum negotium huc redit, ut, ponendo brevitatis gratia $-fg=r$, ostendatur, si formula r^p-1 fuerit divisibilis per $2p+1$, tum etiam hanc formulam: $r^{p+2nr}-1$ fore divisibilem per $2p+1+4nr$, siquidem numerus $2p+1+4nr$ fuerit numerus primus.

§ 43. **Coroll. 3.** Si ponamus $r=-1$, evidens est formulam -1^p-1, dividi non posse per $2p+1$, nisi p sit numerus par. Sit ergo $p=2q$ et $4q+1$ numerus primus, tum certe inter residua reperietur $4q$. Sit quadratum, unde hoc residuum nascitur $=vv$, et $vv+1$ divisibile erit per $4p+1$. Ita ex his rationibus facillime patet, semper dari summam duorum quadratorum divisibilem per numerum $4q+1$, id quod alias per multas demum ambages ostendi solet.

§ 44. Missis autem his, quae principiis nondum satis corroboratis innituntur, per certa principia in indolem hujusmodi aequationum: $fxx+gyy=szz$, accuratius inquiramus. Ac primo

quidem jam rigorose monstravimus, si haec aequatio possibilis fuerit casu $s=h$, tum sumto numero k, ita ut sit $pp+fgqq=krr$, fore etiam $s=hk$ valorem idoneum pro s. Hoc igitur praemisso ad sequentia progrediamur.

§ 45. **Theorema 1.** Si aequatio $fxx+gyy=hzz$ fuerit possibilis, tum semper assignari potest talis formula: $tt+fg$, per numerum h divisibilis, ita ut numerus t minor sit quam $\frac{1}{2}h$.

Demonstratio. Quum formula illa $fxx+gyy$ divisibilis sit per h, si ea ducatur in formulam $fpp+gqq$, etiam productum per h erit divisibile. Sumantur ergo numeri p et q ita, ut sit $py-qx=1$, id quod semper fieri potest, nisi x et y habeant communem divisorem, qui autem casus hinc sponte excluditur; tum autem productum illud erit

$$(fpx+gqy)^2+fg,$$

unde sumto $t=fpx+gqy$ formula $tt+fg$ divisorem habebit h. Hic autem ponamus $t=t'\pm\lambda h$, atque tum haec formula $t't'+fg$ etiamnunc per h erit divisibilis. Hoc vero modo t' infra semissem numeri h deprimetur, consequenter certo dabitur formula $tt+fg$ divisibilis per h, in qua t non excedit semissem ipsius h.

§ 46. **Coroll. 1.** Haec eadem proprietas numeri h, quia tantum a producto fg pendet, aeque patet ad hanc aequationem: $xx+fgyy=hzz$. Quin etiam, si productum fg in duos alios factores ζ et η resolvi queat, eadem conditio locum habet, ut aequatio $\zeta xx+\eta yy=hzz$ sit possibilis.

§ 47. **Coroll. 2.** Quoties ergo numerus h fuerit divisor formulae $tt+fg$, inde non semper concludi potest, aequationem $fxx+gyy=hzz$ esse possibilem, sed plus inde inferri nequit, quam dari formulam affinem $\zeta xx+\eta yy$ aequalem termino hzz, dummodo fuerit $\zeta\eta=fg$.

§ 48. **Coroll. 3.** Quia $t<\frac{1}{2}h$, formula $tt+fg$ minor erit quam $\frac{1}{4}hh+fg$, quae ergo si dividatur per h, quotus minor erit quam $\frac{1}{4}h+\frac{fg}{h}$.

§ 49. **Coroll. 4.** Vicissim ergo etiam patet, si nulla detur hujusmodi formula per h divisibilis, tum etiam neque hanc aequationem: $fxx+gyy=hzz$, neque ullam aliam affinem

$$\zeta xx+\eta yy=hzz$$

esse possibilem, si scilicet fuerit $\zeta\eta=fg$. Ad hoc ergo examinandum sufficit eos tantum casus evolvisse, quibus $t<\frac{1}{2}h$.

§ 50. **Theorema 2.** Si aequatio $fxx+gyy=hzz$ fuerit possibilis, tum semper numerum h', minorem quam h, exhibere licet, ita ut haec aequatio: $fxx+gyy=h'zz$, sit possibilis.

Demonstratio. Si ponamus formulam $tt+fg=k$, supra jam demonstravimus, etiam hanc formam: $fxx+gyy=hkzz$ esse possibilem. Modo autem vidimus pro t dari valorem adeo minorem quam $\frac{1}{2}h$, quo formula $tt+fg$ habeat factorem h. Sit ergo alter factor h', ideoque $k=hh'$ et $hk=h'h^2$, et deleto quadrato hh, utpote in quadrato zz involvendo, orietur aequatio quoque possibilis:

$$fxx+gyy=h'zz, \quad \text{ubi } h'<\tfrac{1}{4}h+\tfrac{fg}{h}.$$

§ 51. **Coroll. 1.** Quantuscunque ergo fuerit numerus h', hoc modo continuo ad minores valores h', h'', etc. pervenire licebit, donec tandem numeri prodeant tam parvi, qui ulteriorem diminutionem non admittunt. Quia enim $h' < \frac{1}{2}h + \frac{fg}{h}$, utique h' excedere debebit $\frac{fg}{h}$; unde manifestum est, quo minor numerus h fuerit redditus, ulteriorem diminutionem retardari, atque adeo penitus sisti.

§ 52. **Coroll. 2.** Si, dum hoc modo pro h continuo minores valores eruuntur, tandem perveniatur ad valorem vel f, vel g, hinc certo concludere poterimus, aequationem propositam esse possibilem, quandoquidem ista: $fxx + gyy = fzz$ casum maxime obvium involvit, scilicet $y = 0$ et $z = x$. Sin autem nullo modo deducamur ad f vel g, sed ad alium numerum ζ, divisorem ipsius fg, indicio id erit, non ipsam aequationem propositam, sed aliam affinem, scilicet $\zeta xx + \eta yy = hzz$ esse possibilem; unde si tandem adeo perveniretur ad unitatem, tum aequatio $xx + fgyy = hzz$ foret possibilis.

§ 53. **Problema.** Proposita aequatione $fxx + gyy = hzz$, investigare, utrum ea sit possibilis, nec ne?

Solutio. Quia hic tres numeri proponuntur, f, g et h, aequatio ita exhibeatur, ut numerus h eorum sit maximus, quandoquidem hic perinde est, utrum termini aequationis sint positivi, an negativi. Tum sumatur formula $tt + fg$, et examen instituatur, utrum, pro t numeris minoribus quam $\frac{1}{2}h$ sumendis, haec formula fiat divisibilis per h, nec ne? Casu posteriore statim pronunciare poterimus, aequationem propositam esse possibilem; priore autem casu loco h nanciscemur alium numerum minorem h' simili modo examini subjiciendum, donec tandem ulterior diminutio non habeat locum. Et si inter hos valores occurrat f vel g, certum hoc erit indicium, aequationem propositam esse possibilem; sin autem ad alium numerum ζ, divisorem producti fg, perveniamus, tum concludemus, aequationem $\zeta xx + \eta yy = hzz$ esse possibilem, existente $\zeta\eta = fg$. Quodsi autem neutrum usu veniat, tum in valore minimo in locum h succedente aequiescamus, qui sit h', et nunc aequationem $fxx + gyy = h'zz$ ita disponamus, ut litterarum f et g major, puta g, ad dextram referatur hoc modo: $h'zz - fxx = gyy$, et nunc loco g simili modo quaerantur g', donec perveniatur ad g', sive ipsi h', sive ipsi f aequalem, quo casu propositum nostrum itidem erit evictum. At si ne hoc quidem facile patescat, loco g introducamus valorem exiguum inde ortum g', et nunc aequatio $h'zz - g'yy = fxx$ simili modo tractetur; sicque tandem ad ternos numeros f', g', h' pervenietur, ut judicium nulla amplius difficultate laborare possit.

§ 54. **Coroll. 1.** Si numerus h fuerit praegrandis, utique taedioso calculo erit opus, antequam formulae $tt + fg$ omnes casus usque ad $t = \frac{1}{2}h$ exigantur; vix autem talem laborem quisquam suscipiet. Admisso autem superiore principio, statim valor iste h infra $4fg$ deprimetur.

§ 55. **Coroll. 2.** Si ingens ille numerus h habeat factores, puta m et n, hic labor non parum sublevabitur, dum primo talis valor pro t investigatur, ut formula $tt + fg$ saltem divisibilis fiat vel per m, vel per n; neque enim deinceps difficile erit casum elicere, quo ista formula per ipsum numerum h fiat divisibilis. De cetero tota haec operatio exemplis clarius illustrabitur.

§ 56. **Exempl. 1.** Examinanda proponatur haec aequatio: $3xx + 5yy = 1007zz$. Sumatur ergo formula $tt + 15$, ob $f = 3$ et $g = 5$, et quia $h = 1007 = 19.53$, quaeratur t primo ita, ut $tt + 15$ saltem divisorem obtineat 19, quod manifesto fit sumendo $t = 2$; tum enim fit $k = 19$, et sic prodit $h' = 53$, sublato quadrato 19^2. Nunc porro quaeratur t, ut formula $tt + 15$ divisorem nasciscatur 53, quod fit si $t = 12$, ita ut jam habeamus $k = 159 = 3.53$, ideoque $h'k = 3.53^2$, sicque $h'' = 3$, qui numerus, quum aequalis sit ipsi f, indicat nostram formulam esse possibilem.

§ 57. **Exempl. 2.** Proponatur haec aequatio: $2xx + 7yy = 23zz$. Hic $f = 2$, $g = 7$ et $h = 23$. Sumatur $k = tt + 14$, qui numerus fit divisibilis per 23, sumendo $t = 3$. Erit autem $k = 23h$, ideoque $hk = 23^2$; unde intelligimus, hanc aequationem: $xx + 14yy = zz$ esse possibilem; neque vero hinc sequitur propositam esse impossibilem, quum fieri possit, ut utraque simul locum habeat. Videamus ergo an haec forma: $2xx + 7yy = zz$ sit possibilis, quod quidem manifestum est sumendo $x = 1$, $y = 1$ et $z = 3$. Sed tamen regula nostra utamur, et quia est $h' = 1$, sumendo $t = 2$, erit $k = 18 = 2.3^2$, hinc $h'k = 2.3^2$, ideoque $h'' = 2$, hoc est $h'' = f$; sicque patet etiam ipsam propositam aequationem esse possibilem.

§ 58. **Coroll.** Quum ergo hoc casu utraque forma $fxx + gyy = hzz$ et $xx + fgyy = hzz$ sit possibilis, operae pretium erit in eos casus inquirere, quibus utraque formula $fxx + gyy$ et $xx + fgyy$ eidem termino hzz aequalis esse possit. Hoc autem manifesto eveniet, quando fieri poterit $fxx + gyy = uu + fgvv$, quod si evenire possit, infiniti certe exhiberi poteruut casus, inter quos dabitur unus, quo $v = 0$. Illud igitur evenit, quoties evadere potest $fxx + gyy = uu$, id quod nostro exemplo manifesto fit.

§ 59. **Exempl. 3.** Proponatur aequatio $xx + 6yy = 145zz = 5.29zz$. In formula ergo $k = tt + 6$ sumamus $t = 2$, ut fiat $k = 2.5$, ideoque $hk = 2.5^2.29$, sicque $h' = 2.29$. Nunc sumatur t ita, ut k fiat per 29 divisibile, quod evenit sumendo $t = 9$: fiet enim $k = 87 = 3.29$, ergo $h'k = 2.3.29^2$ et $h'' = 6 = g$, consequenter nostra aequatio est utique possibilis.

§ 60. **Exempl. 4.** Proponatur aequatio: $3xx + 7yy = 89zz$. Hic est $f = 3$, $g = 7$ et $h = 89$, ideoque $k = tt + 21$. Quaeratur ergo t, ut illa formula divisibilis fiat per 89. Ponamus in hunc finem $tt + 84 = 89n$. Hic enim loco 21 scribere liceret $21uu$ in genere, atque hic sumsimus $u = 2$, ut etiam hunc casum illustramus. Quum autem nullum quadratum sit formae $3n + 2$, pro numero n excluduntur valores 1, 4, 7, 10, et in genere $3\alpha + 1$. Deinde excluduntur omnes numeri impariter pares 2, 6, 10, 14, etc. et quia omnia quadrata sunt formae vel $5\alpha + 3$, vel $5\alpha + 4$, pro n etiam excluduntur hi numeri: 3, 4, 8, 9, 13, 14, et in genere $5\alpha + 3$ et $5\alpha + 4$. His exclusis pro n remanent examinandi hi numeri: 5, 11, 12, 15, 17, 20, 21, 27, 32, 35, 36, 41, quos ergo successive in aequatione $tt = 89n - 84$ loco n substitui oportet. At vero primus valor $n = 5$ statim praebet quadratum, unde $k = 5.89$ et $h' = 5$. Nunc autem k per 5 fiet divisibile sumendo $t = 1$, unde fit $k = 5.17$ et $h'' = 17$. Quia ergo neque ad 3, neque ad 7 pervenimus, sumto $h' = 5$ examinemus aequationem $5zz - 3xx = 7yy$, atque jam tota operatio est mutanda, dum habemus $f = 5$, $g = -3$ et $h = 7$, quocirca, posito $k = tt - 15$, sumamus $t = 1$, ut fiat $k = -2.7$, unde fit $h' = -2$, ita ut nunc aequatio examinanda sit haec $5zz - 3xx = -2yy$, sive $3xx - 2yy = 5zz$, ubi $f = 3$. $g = -2$ et $h = 5$. Sumto ergo

$k = tt - 6$, fiat $t = 1$, erit $k = -5$ et $h' = -1$, ergo pervenimus ad hanc aequationem: $3xx - 2yy = -zz$, sive $2yy - zz = 3xx$, ubi habemus $f = 2$, $g = -1$, $h = 3$. Erit ergo $k = tt - 2$, quod cum nullo modo fieri possit, omnes istae aequationes, ideoque et ipsa proposita sunt impossibiles.

§ 61. **Exempl. 5.** Sit proposita aequatio $3xx + 7yy = 178zz$, ubi ut antea $f = 3$, $g = 7$, at $h = 178 = 2.89$, duplo major quam casu precedente. Posito ergo $k = tt - 21$, ex praecedente patet pro t sumi debere 23. Posito igitur $tt = 81n - 21$, pro n relinquuntur numeri:

5, 8, 9, 14, 18, 20, 24, 29, 30, 33, 38, 44.

Reperitur autem $n = 14$, unde fit $t = 35$, sicque erit $k = 14.89$, hincque $h' = 2.14 = 4.7$, ideoque $h' = 7$, qui numerus quum ipsi numero g sit aequalis, indicat aequationem nostram esse possibilem.

§ 62. **Problema.** Postquam aequatio $fxx + gyy = hzz$ methodo praecedente possibilis fuerit inventa, dum tandem valores ex h inventi perducti fuerint ad f, sive ad g, determinare ipsa quadrata xx et yy, quibus aequatio evadit possibilis.

Solutio. Quia solutio praecedens ad sequentes formulas est perducta:

$$k = aa + fg = hh'; \quad k' = bb + fg = h'h''; \quad k'' = cc + fg = h''h'''; \text{ etc.}$$

habebimus $hk = h^2h' = h'.\square$, hincque $hk^2 = h'k.\square$. Simili modo reperiemus $h'.\square = h''k'$, item $h''.\square = h'''k''$, etc. Sit nunc $h''' = f$, erit $h'' = f.k''$, hinc $h'.\square = f.k''.k'$, ac tandem $h.\square = f.k.k'.k''$, consequenter habebimus $h.\square$, hoc est

$$hzz = f(aa + fg)(bb + fg)(cc + fg)(dd + fg) \text{ etc.}$$

quod productum manifesto reducitur ad $f(A^2 + fgB^2)$, ita ut hinc fiat $hzz = fA^2 + ffgB^2$, quocirca nanciscimur $x = A$ et $y = fB$, sicque problema est resolutum.



XLI.

De resolutione irrationalium per fractiones continuas, ubi simul nova quaedam et singularis species minimi exponitur.

(N. Comment. XVIII. 1773 p. 218. Exhib. 1772 Dec. 10).

1. In superiore dissertatione (XXXIX pag. 549) de resolutione aequationis

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0,$$

totum negotium praecipue ad hanc quaestionem erat deductum, ut pro litteris x et y valores in numeris integris investigentur, quibus formulae $Ax^2 + 2Bxy + Cy^2$ minimus valor inducatur. Tres autem hic potissimum considerandi sunt casus, prouti haec formula vel duos factores habet imaginarios, quod fit si $BB - AC$ fuerit numerus negativus, vel factores inter se aequales, quod fit si $BB - AC = 0$, vel denique si ejus factores fuerint reales, quod fit si $BB - AC$ numerus positivus. Primo autem casu haec quaestio minimi nullam attentionem meretur, quoniam solutio nulla plane difficultate laborat. Secundus vero casus multo minus negotium facessit, quum formula abeat in quadratum, cujus radicem facillime minimam reddere licet. Solus ergo tertius casus superest, qui accuratiorem investigationem postulat, unde quidem insuper excludi convenit casus, quibus formula $BB - AC$ est numerus quadratus, et ambo factores adeo rationales evadunt, tum enim valor formulae propositae adeo ad nihilum redigi poterit, ita ut quaestio minimi hic ne locum quidem habeat.

2. Soli ergo nobis relinquuntur casus, quibus numerus $BB - AC$ est numerus positivus sed non quadratus, cujusmodi est ista formula: $mxx - nyy$, denotantibus litteris m et n numeros integros positivos, ejusmodi tamen, ut non uterque sit quadratus; tum enim evidens est istam formulam ad nihilum reduci non posse, nisi tam x quam y evanescat, quem casum tamen utpote obvium excludi oportet. Cum ergo haec formula $mxx - nyy$ ad nihilum redigi se non patiatur, quaestio sine dubio notatu digna est censenda, qua litterarum x et y ii valores in integris quaeruntur, quibus ipsa formula $mxx - nyy$ minimum omnium adipiscatur valorem. Si alter numerorum m et n unitati aequetur, semper formulam ad unitatem usque deprimere licebit, qui certe est minimus valor, cyphra excepta. Si enim fuerit $m = 1$ ex theoremate Pelliano notissimo constat, semper effici posse

$$xx - nyy = 1, \quad \text{sive} \quad x = \sqrt{(nyy + 1)},$$

dummodo n non fuerit numerus quadratus, atque adeo hoc non solum unico modo praestari potest, sed etiam infinitis, quemadmodum jam ab ipso Pellio est demonstratum. Sin autem alter numerus n unitati aequetur, formula $mxx - nyy$ hac methodo ad -1 deprimitur, qui casus aeque pro minimo est habendus ac $+1$, dum in ea investigatione, quae ad hanc quaestionem ansam dedit, discrimen signi non spectatur.

3. His ergo casibus remotis, quo alter numerus m vel n unitati aequatur, quaestio nostra potissimum versatur circa formulam $mxx - nyy$, quippe ad quam semper formulam generalem $Axx - 2Bxy + Cyy$ revocare licet. Si enim in genere statuatur $x = t + Bu$ et $y = Au$, facta substitutione formula generalis abit in hanc formam: $Att - A(BB - AC)uu$ sicque formula nostra assumta $mxx - nyy$ aeque late patere est censenda, atque ipsa proposita trinomialis. Etiamsi autem neque m, neque n unitati aequetur, saepenumero usu venire potest, ut formulam nostram quoque ad unitatem usque deprimere liceat; idque vel statim manifesto occurrit, veluti in hac forma: $3xx - 2yy$, quae ad unitatem redigitur sumtis $x = 1$ et $y = 1$, vel non statim se offert, uti fit in $9xx - 5yy$, quae posito $x = 3$ et $y = 4$ ad unitatem redit; quicquid autem sit, utique evenire potest, ut minimus valor nostrae formulae unitatem excedat, ac tum judicium de minimo plerumque summis difficultatibus involutum deprehenditur, ceu fit in hac formula $13xx - 7yy$, quam usque ad binarium deprimi posse non facile perspicitur, si scilicet ponatur $x = 15$ et $y = 11$. At si m et n fuerint numeri praegrandes, judicium multo operosiores calculos requirit, quamobrem methodus certa etiam in his casibus minimum investigandi analysin haud contemnendo incremento locupletare videtur.

4. Antequam autem hanc ipsam methodum explicare adgrediar, plurimum ostendisse juvabit, semper infinitis modis idem minimum obtineri posse. Atque hoc adeo generalius ita demonstrari potest: Quodsi unicus casus constet, quo formula $mxx - nyy$ aequalis fiat dato numero k, tum semper infiniti valores pro x et y reperiri possunt, qui ad eundem numerum k deducant. Sit enim casu illo cognito $x = a$ et $y = b$, ita ut sit $maa - nbb = k$, et nunc numeros x et y ita definiri oportet, ut fiat $mxx - nyy = maa - nbb$, id quod sequenti modo commodissime praestabitur. Ante omnia quaerantur numeri p et q, ut fiat $pp - mnqq = 1$, id quod infinitis modis semper fieri posse constat, dummodo mn non fuerit numerus quadratus, uti hic assumimus, atque nunc quaesito satisfieri manifestum est, si statuatur

$$mxx - nyy = (maa - nbb)(pp - mnqq)^2;$$

quod quo facilius fieri possit, sumamus factores etsi irrationales et ponamus

$$x\sqrt{m} + y\sqrt{n} = (a\sqrt{m} + b\sqrt{n})(p + q\sqrt{mn})^2.$$

tum enim mutato signo radicalis $\sqrt{n}$, sponte fiet

$$x\sqrt{m} - y\sqrt{n} = (a\sqrt{m} - b\sqrt{n})(p - q\sqrt{mn})^2,$$

sicque alteri tantum harum duarum aequationum satisfecisse sufficiet. Quia autem evolutio formulae $(p + q\sqrt{mn})^2$ alternatim terminos rationales et irrationales radicali $\sqrt{mn}$ affectos praebet, sit P summa terminorum rationalium et $Q\sqrt{mn}$ summa irrationalium, ita ut sit

$$(p + q\sqrt{mn})^2 = P + Q\sqrt{mn},$$

similique modo

$$(p - q\sqrt{mn})^2 = P - Q\sqrt{mn}.$$

Nunc igitur aequatio nostra erit

$$x\sqrt{m} + y\sqrt{n} = (a\sqrt{m} + b\sqrt{n})(P + Q\sqrt{mn}),$$

sive

$$x\sqrt{m} + y\sqrt{n} = (aP + nbQ)\sqrt{m} + (bP + maQ)\sqrt{n},$$

ubi tam partes signo $\sqrt{n}$, quam partes signo $\sqrt{m}$ affectae seorsim sunt inter se aequandae, atque hinc statim elicimus sequentes valores.

$$x = aP + nbQ, \qquad y = bP + maQ,$$

simulque patet multitudinem harum solutionum revera esse infinitam.

5. His praemissis ipsam nostram quaestionem adgrediamur, quaesituri valores litterarum x et y, quibus formula $mxx - nyy$ minimum sortiatur valorem, qui sit $= k$, ac statim quidem evidens est his casibus formulam $mxx - nyy$ propius ad nihilum redigi, quam ullis aliis casibus, sicque pro x et y ejusmodi investigandi sunt valores, quibus proxime fiat $\frac{x}{y} = \sqrt{\frac{n}{m}} = \frac{\sqrt{mn}}{m}$, quocirca negotium jam huc est perductum, ut quaerantur fractiones rationales $\frac{x}{y}$, quae tam prope aequentur formae irrationali $\frac{\sqrt{mn}}{m}$, quam quidem fieri potest, non majoribus numeris pro x et y adhibendis.

6. Hoc autem problema jam olim a Wallisio propositum expeditissime resolvitur, si formula $\frac{\sqrt{mn}}{m}$ in fractionem continuam convertatur, simili scilicet operatione, qua vulgo maximus communis divisor duorum numerorum quaeri solet. Si enim hoc modo perventum fuerit ad hanc fractionem continuam:

$$\frac{\sqrt{mn}}{m} = \alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \cfrac{1}{\delta + \cfrac{1}{\varepsilon + \text{etc.}}}}}$$

continui hi quoti in seriem disponantur, ac primo quidem ipsi α subscribatur fractio $\frac{1}{0}$, ipsi β vero $\frac{\alpha}{1}$, ac deinceps ex binis fractionibus continuo sequens formatur, dum ultimae tam numerator quam denominator per indicem supra scriptum multiplicetur, hisque productis tam numerator quam denominator penultimae fractionis respective addantur; sequenti scilicet modo

$$\begin{array}{cccccc} \alpha, & \beta, & \gamma, & \delta, & \varepsilon, & \\ \frac{1}{0}, & \frac{\alpha}{1}, & \frac{\alpha\beta+1}{\beta}, & \frac{\alpha\beta\gamma+\gamma+\alpha}{\beta\gamma+1}, & \frac{\alpha\beta\gamma\delta+\gamma\delta+\alpha\delta+\alpha\beta+1}{\beta\gamma\delta+\delta+\beta}, & \text{etc.} \end{array}$$

7. Omnes istae fractiones hac gaudent proprietate, ut quaelibet valorem formulae $\frac{\sqrt{mn}}{m}$ propius exhauriat, quam fieri poterit numeris non majoribus adhibendis. Verum etiam inter has ipsas fractiones ingens intercedit discrimen, quod aliae aliis, ceteris quidem paribus magis adpropinquent. Eae autem maxime adpropinquare sunt compertae, quae maximos indices sibi habent inscriptos; si ergo illae pro $\frac{x}{y}$ accipiantur, jam certi sumus istis numeris pro x et y assumtis, formulae nostrae $mxx - nyy$ minimum valorem induci. Simul vero notari oportet inter hos quotos successivos α, β, γ, δ, ε, etc. semper dari periodos, in quibus idem quotorum ordo recurrit, omnes ergo fractiones iisdem maxime quotis suscriptae omnes quoque valores idoneos pro x et y suppeditabunt, quibus formula nostra $mxx - nyy$ eundem minimum valorem nanciscitur.

8. Quo autem operationes, quibus isti quoti facillime eruuntur, clarius explicare valeam, exemplum primo determinatum expediamus, quo formula proposita sit $7xx - 13yy$, ita ut jam proxime fieri debeat $\frac{x}{y} = \frac{\sqrt{91}}{7}$, ubi tantum notetur esse $\sqrt{91} > 9$ et < 10. Nunc ergo operatio uti pro maximo divisore instituatur: ac primo dividi oportet $\sqrt{91}$ per 7, unde primus quotus prodit $= 1$,

residuum vero $= \sqrt{91} - 7$, per quod praecedens disivor 7 debet dividi; multiplicetur uterque numerus per $\sqrt{91} + 7$, ac divisor jam erit 42, dividendus autem $7(\sqrt{91} + 7)$, qui per septenarium depressi, praebent divisorem $= 6$ et dividendum $= \sqrt{91} + 7 > 16$, unde secundus quotus colligitur 2, ac residuum fiet $\sqrt{91} - 5$, per quod 6 debet dividi. Multiplicando per $\sqrt{91} + 5$, divisor erit 66 et dividendus $6(\sqrt{91} + 5)$, ac per 6 deprimendo, jam per 11 dividi debet $\sqrt{91} + 5$, unde tertius quotus fit 1, residuo manente $\sqrt{91} - 6$, per quod praecedens divisor 11 debet dividi. Quae operatio ulterius hic repraesentatur

$\frac{11}{\sqrt{91}-6}$	multipl.	per	$\sqrt{91}+6$,	fit	$\frac{11(\sqrt{91}+6)}{55}$	divid.	per	11,	fit	$\frac{\sqrt{91}+6}{5}$	quot 3 (*N.* 4),
$\frac{5}{\sqrt{91}-9}$	«	«	$\sqrt{91}+9$,	«	$\frac{5(\sqrt{91}+9)}{10}$	«	«	5,	«	$\frac{\sqrt{91}+9}{2}$	« 9 (*N.* 5),
$\frac{2}{\sqrt{91}-9}$	«	«	$\sqrt{91}+9$,	«	$\frac{2(\sqrt{91}+9)}{10}$	«	«	2,	«	$\frac{\sqrt{91}+9}{5}$	« 3 (*N.* 6),
$\frac{5}{\sqrt{91}-6}$	«	«	$\sqrt{91}+6$,	«	$\frac{5(\sqrt{91}+6)}{55}$	«	«	5,	«	$\frac{\sqrt{91}+6}{11}$	« 1 (*N.* 7),
$\frac{11}{\sqrt{91}-5}$	«	«	$\sqrt{91}+5$,	«	$\frac{11(\sqrt{91}+5)}{66}$	«	«	11,	«	$\frac{\sqrt{91}+5}{6}$	« 2 (*N.* 8),
$\frac{6}{\sqrt{91}-7}$	«	«	$\sqrt{91}+7$,	«	$\frac{6(\sqrt{91}+7)}{42}$	«	«	6,	«	$\frac{\sqrt{91}+7}{7}$	« 2 (*N.* 9),
$\frac{7}{\sqrt{91}-7}$	«	«	$\sqrt{91}+7$,	«	$\frac{7(\sqrt{91}+7)}{42}$	«	«	7,	«	$\frac{\sqrt{91}+7}{6}$	« 2 (*N.* 10).

Ulterius calculum producere non est opus, quia haec postrema divisio cum secunda convenit et jam periodus secunda incipit; ubi notandum loco primi quoti 1 hic ejus duplum occurrere, id quod in hujusmodi divisionibus semper usu venit.

9. Quoti ergo ordine inventi sequenti modo progrediuntur:

1, 2, 1, 3, 9, 3, 1, 2, 2, 2, 1, 3, 9, 3, 1, 2,

inter quos maxime eminent 9, ideoque nullum amplius est dubium, quin illae fractiones, quae his quotis subjiciuntur, formulae $7xx - 13yy$ omnium valorum minimum concilient. Adponamus igitur has fractiones sequenti modo

$$\begin{array}{ccccc} 1, & 2, & 1, & 3, & 9, \\ \frac{1}{0}, & \frac{1}{1}, & \frac{3}{2}, & \frac{4}{3}, & \frac{15}{11}, \end{array}$$

unde patet fractionem nobis satisfacientem fore $\frac{x}{y} = \frac{15}{11}$, sive $x = 15$ et $y = 11$. Hinc autem $7xx = 1575$ et $13yy = 1573$, unde minimus valor sine ullo dubio est binarius, quem divinando non tam facile quisquam detexerit.

10. Si has operationes, quibus illi quoti continui reperiuntur, attentius perpendamus, calculum non mediocriter contrahi posse facile perspicere licet. Sit enim $\sqrt{k}$ quantitas illa irrationalis, quam formula in fractionem continuam convertenda involvit, numerus autem integer proxime minor quam $\sqrt{k}$ sit $= e$, et ponamus perventum jam esse ad divisionem, qua formula $\sqrt{k} + r$ dividi debet per numerum p, ita ut quotus hinc oriundus sit $q < \frac{e+r}{p}$, eritque residuum $= \sqrt{k} + r - pq$, et quia $pq > r$ (saltem quando operationes jam ordine progrediuntur), vocemus $pq - r = r'$, ita ut jam residuum sit $\sqrt{k} - r'$, unde pro sequente divisione habebimus divisorem $= \sqrt{k} - r'$ et dividendum

$=p$, multiplicetur uterque per $\sqrt{k}+r'$ et fiat $\frac{k-r'r'}{p}=p'$ (vidimus enim semper in decursu operationum, formulam $k-r'r'$ divisibilem fore per p), et jam sequens divisio ita erit comparata, ut sit divisor $=p'$ et dividendus $\sqrt{k}+r'$, unde nascetur quotus $q'<\frac{e+r'}{p'}$, atque hinc simili modo tertia et sequentes divisiones conficientur.

11. Ex prima igitur illa operatione, qua formulam $\sqrt{k}+r$ dividi oportet per numerum p, notentur tantum numeri r et p, unde deducitur quotus $q<\frac{e+r}{p}$, deinde sumatur $r'=pq-r$ et $p'=\frac{k-r'r'}{p}$, hincque fiet $q'<\frac{e+r'}{p'}$, simili modo capiatur porro $r''=p'q'-r'$ et $p''=\frac{k-r''r''}{p'}$, hincque $q''<\frac{e+r''}{p''}$. Quas operationes sequente schemate repraesentamus:

r,	p,	$q<\frac{e+r}{p}$,
$r'=pq-r$,	$p'=\frac{k-r'r'}{p}$,	$q'<\frac{e+r'}{p'}$,
$r''=p'q'-r'$,	$p''=\frac{k-r''r''}{p'}$,	$q''<\frac{e+r''}{p''}$,
$r'''=p''q''-r''$,	$p'''=\frac{k-r'''r'''}{p''}$,	$q'''<\frac{e+r'''}{p'''}$,
etc.	etc.	etc.

Hocque modo progressio quotorum q, q', q'', q''', etc. facillime inveniri posse videtur.

12. Dilucidemus hanc regulam exemplo, quo formula $5xx-38yy$ minimum sit reddenda, seu fractio $\frac{x}{y}=\frac{\sqrt{38}}{\sqrt{5}}=\frac{\sqrt{190}}{5}$ per fractionem infinitam evolvenda. Hic igitur erit $k=190$, $e=13$, $p=5$ et $r=0$, unde totus calculus sequenti modo instituetur:

$r=0$,	$p=5$,	$q=2<\frac{13+0}{5}$,
$r'=10$,	$p'=\frac{190-100}{5}=18$,	$q'=1<\frac{13+10}{18}$,
$r''=8$,	$p''=\frac{190-64}{18}=7$,	$q''=3<\frac{13+8}{7}$,
$r'''=13$,	$p'''=\frac{190-169}{7}=3$,	$q'''=8<\frac{13+13}{3}$,
$r^{IV}=11$,	$p^{IV}=\frac{190-121}{3}=23$,	$q^{IV}=1<\frac{13+11}{23}$,
$r^{V}=12$,	$q^{V}=\frac{190-144}{23}=2$,	$q^{V}=12<\frac{13+12}{2}$,
$r^{\cdots}=12$,	$p^{\cdots}=\frac{190-144}{2}=23$,	$q^{\cdots}=1<\frac{13+12}{23}$,
$r^{\cdots}=11$,	$p^{\cdots}=\frac{190-121}{23}=3$,	$q^{\cdots}=8<\frac{13+11}{3}$,
$r^{\cdots}=13$,	$p^{\cdots}=\frac{190-169}{3}=7$,	$q^{\cdots}=3<\frac{13+13}{7}$,
$r^{\cdots}=8$,	$p^{\cdots}=\frac{190-64}{7}=18$,	$q^{\cdots}=1<\frac{13+8}{18}$,
$r^{\cdots}=10$,	$p^{\cdots}=\frac{190-100}{18}=5$,	$q^{\cdots}=4<\frac{13+10}{5}$,
etc.	etc.	etc.

Calculum ulterius prosequi non est opus, quum jam patescat quotorum ordo

2, 1, 3, 8, 1, 12, 1, 8, 3, 1 4, 1, 3, 8, 1, 12, 1, 8, etc.

unde fractio continua oritur

$$\frac{x}{y} = \sqrt{\frac{38}{5}} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{8 + \cfrac{1}{1 + \cfrac{1}{12 + \cfrac{1}{1 + \cfrac{1}{8 \text{ etc.}}}}}}}}$$

Tum vero quum maximus horum quotorum sit 12, ei respondebit valor minimus formulae propositae $5xx - 38yy$, at fractio $\frac{x}{y}$ ita definietur

2,	1,	3,	8,	1,	12
$\frac{1}{0}$,	$\frac{2}{1}$,	$\frac{3}{1}$,	$\frac{11}{4}$,	$\frac{91}{38}$,	$\frac{102}{37}$,

sicque pro casu minimi habemus $x = 102$ et $y = 37$, unde $5xx = 52020$ et $38yy = 52022$, ergo differentia $= -2$, quia autem inter quotos etiam eminet 8, eique subjacet fractio $\frac{11}{4}$, sumendo $x = 11$ et $y = 4$, colligitur valor formulae $5xx - 38yy = 605 - 608 = -3$, qui valor post illum sine dubio est minimus.

13. Plura hujus generis exempla non afferimus, sed quo haec methodus succincta ad usum ampliorem accommodetur, investigemus fractiones continuas pro singulis multiplis ipsius $\sqrt{2}$; plurimum enim juvabit, relationem inter hos valores perpendisse, siquidem hoc argumentum de fractionibus continuis neutiquam adhuc satis est exploratum. Quotos autem tantum pro singulis his multiplis adposuisse sufficiet:

pro $\sqrt{2}$....quoti	1,	2,	2,	2,	2.	2	
pro $2\sqrt{2}$...quoti	2,	1,	4,	1,	4,	1,	4
pro $3\sqrt{2}$...quoti	4,	4,	8,	4,	8,	4,	8
pro $4\sqrt{2}$...quoti	5,	1,	1,	1,	10,	1,	1
pro $5\sqrt{2}$...quoti	7,	14,	14,	14,	14,	14,	14
pro $6\sqrt{2}$...quoti	8,	2,	16,	2,	16,	2,	16
pro $7\sqrt{2}$...quoti	9,	1,	8,	1,	18,	1,	8.

14. Hae progressiones eo magis sunt notatu dignae, quod tantopere a se invicem discrepant, etiamsi ipsae quantitates iis expressae tam simplicem rationem inter se teneant. Neque vero tantum multipla tantam gignunt differentiam in fractionibus continuis, sed etiam ipsa additio adhuc majus discrimen parit, si scilicet ad $\sqrt{2}$ quaepiam fractio rationalis addatur; id quod exemplo formulae $\frac{1}{2} + \sqrt{2}$ illustremus, ubi adeo usu venit, ut primae operationes peculiarem evolutionem requirant, dum quotos a sequentibus periodis diversos praebent. Ponatur ergo

$$\frac{x}{y} = \frac{1 + 2\sqrt{2}}{2} = \frac{1 + \sqrt{8}}{2}.$$

Primo igitur per 2 dividatur $1 + \sqrt{8}$ et quotus erit 1; residuum vero $\sqrt{8} - 1$, per quod dividi debet 2, multiplicetur utrinque per $\sqrt{8} + 1$, ut per 7 dividi debeat $2\sqrt{8} + 2 = \sqrt{32} + 2$, et nunc operatio in ordinem subit, hic scilicet est $k = 32$, $e = 5$, $r = 2$ et $p = 7$ et operationes ita se habebunt:

$r = 2$	$p = 7$	$q = 1$
$r = 5$	$p = 1$	$q = 10$
$r = 5$	$p = 7$	$q = 1$
$r = 2$	$p = 4$	$q = 1$
$r = 2$	$p = 7$	$q = 1$
$r = 5$	$p = 1$	$q = 10$
$r = 5$	$p = 7$	$q = 1$
etc.	etc.	etc.

Quum igitur primus quotus fuerit 1 a prioribus prorsus separandus, series quotorum erit:

1, . . 1, 10, 1, 1, 1, 10, 1, . . 1, 10, etc.

quae series eo majorem attentionem meretur, quod a praecedentibus toto coelo discrepat.

15. Sumamus aliud exemplum $\frac{x}{y} = \frac{1}{3} + \sqrt{2} = \frac{1 + \sqrt{18}}{3}$, unde resultat primus quotus $= 1$ et residuum est $\sqrt{18} - 2$, per quod dividi oportet 3, sive multiplicando per $\sqrt{18} + 2$, divisor fit 14, dividendus autem $3\sqrt{18} + 6 = \sqrt{162} + 6$, cujus evolutio sequenti modo repraesentatur:

$$k = 162, \quad e = 12,$$

$r = 6$	$p = 14$	$q = 1$	$r = 6$	$p = 14$	$q = 1$
$r = 8$	$p = 7$	$q = 2$	$r = 8$	$p = 7$	$q = 2$
$r = 6$	$p = 18$	$q = 1$	$r = 6$	$p = 18$	$q = 1$
$r = 12$	$p = 1$	$q = 24$	$r = 12$	$p = 1$	$q = 24$
$r = 12$	$p = 18$	$q = 1$	$r = 12$	$p = 18$	$q = 1$
$r = 6$	$p = 7$	$q = 2$	$r = 6$	$p = 7$	$q = 2$
$r = 8$	$p = 14$	$q = 1$	$r = 8$	$p = 14$	$q = 1$
$r = 6$	$p = 9$	$q = 2$	$r = 6$	$p = 9$	$q = 2$
$r = 12$	$p = 2$	$q = 12$	$r = 12$	$p = 2$	$q = 12$
$r = 12$	$p = 9$	$q = 2$	etc.	etc.	etc.

Series igitur quotorum est

1, . . 1, 2, 1, 24, 1, 2, 1, 2, 12, 2, . . 1, 2, 1, 24, 1, 2, etc.

ubi excluso primo, reliqui secundum denos periodum constituunt.

16. Quum hic sit $\frac{x}{y} = \frac{1 + \sqrt{18}}{3}$, habebimus $3x - y = y\sqrt{18}$; reddamus hanc aequationem rationalem et prodibit

$$9xx - 6xy = 17yy, \quad \text{sive} \quad 9xx - 6xy - 17yy = 0.$$

Hinc ergo discimus, si proposita fuerit haec formula trinomialis $9xx - 6xy - 17yy$, cujusmodi valores litteris x et y tribui debeant, ut haec formula minimum nanciscatur valorem. Scilicet quotis modo inventis subscribantur fractiones more solito, atque ea, cui maximus quotus est inscriptus, dabit valores ipsarum x et y, quocirca has fractiones hic subjiciamus:

$$\begin{matrix} 1, & 1, & 2, & 1, & 24, \\ \frac{1}{0}, & \frac{1}{1}, & \frac{2}{1}, & \frac{5}{3}, & \frac{7}{4}. \end{matrix}$$

Pro casu ergo minimi habemus $\frac{x}{y} = \frac{7}{4}$, sive $x = 7$ et $y = 4$, unde fit

$$9xx = 441, \quad 6xy = 168, \quad 17yy = 272,$$

ergo ipsa formula abit in $+1$, qui valor utique est omnium minimus.

17. Quod si autem hanc formulam modo supra exposito tractare et ad duos terminos redigere vellemus, ob $A = 9$, $B = -3$, $C = -17$, ponendo $x = t + 3u$ et $y = 9u$, prodiret haec formula $9tt - 1458uu = 9(tt - 162uu)$, quae formula certe nunquam minor evadere potest quam 9, ex quo intelligimus, si hujusmodi formularum valores minimos investigare voluerimus, neutiquam licere eas ad duos terminos reducere, quandoquidem hoc modo earum natura penitus mutaretur, quocirca necesse est, tales formulas data opera evolvere; id quod in sequentibus problematibus sumus expedituri.

18. **Problema 1.** *Si formula* $Ax^2 - 2Bxy + Cy^2$ *casu, quo* $x = a$ *et* $y = b$, *praebeat valorem* $= c$, *invenire infinitos alios valores pro* x *et* y, *qui eundem valorem* c *producant, siquidem quantitas* $B^2 - AC$ *fuerit numerus positivus non quadratus.*

Solutio. Quum igitur sit $Aa^2 - 2Bab + Cb^2 = c$,

requiritur, ut fiat $Ax^2 - 2Bxy + Cy^2 = Aa^2 - 2Bab + Cb^2$.

Jam quaerantur ante omnia numeri p et q, ut fiat

$$pp - 2Bpq + ACqq = 1,$$

id quod semper fieri licet, quum hinc sit

$$p = Bq + \sqrt{((B^2 - AC)qq + 1)},$$

cujus resolutio a problemate Pelliano pendet, dummodo $B^2 - AC$ fuerit numerus positivus non quadratus. Statuamus ergo $B^2 - AC = k$, ut fieri debeat

$$p = Bq + \sqrt{(kq^2 + 1)},$$

ita ut quaeri oporteat numerum q, ut formula $kq^2 + 1$ fiat quadratum. Hoc ergo facto statuamus:

$$Ax^2 - 2Bxy + Cy^2 = (Aa^2 - 2Bab + Cbb)(pp - 2Bpq + ACqq)$$

quod productum cum ipsa forma proposita convenire, ita per factores irrationales ostendimus. Quum enim sit

$$Ax^2 - 2Bxy + Cy^2 = \frac{1}{A}(Ax - By + y\sqrt{k})(Ax - By - y\sqrt{k}) \quad \text{et}$$

$$Aa^2 - 2Bab + Cy^2 = \frac{1}{A}(Aa - Bb + b\sqrt{k})(Aa - Bb - b\sqrt{k}) \quad \text{et}$$

$$pp - 2Bpq + ACq^2 = (p - Bq + q\sqrt{k})(p - Bq - q\sqrt{k})$$

statuamus $$Ax - By + y\sqrt{k} = (Aa - Bb + b\sqrt{k})(p - Bq + q\sqrt{k}),$$
tum enim sponte fiet sumendo $\sqrt{k}$ negative
$$Ax - By - y\sqrt{k} = (Aa - Bb - b\sqrt{k})(p - Bq - q\sqrt{k}),$$
unde sufficiet alteram aequationem tantum evolvisse, si modo partes rationales seorsim inter se aequentur. Prodibit igitur
$$Ax - By = (Aa - Bb)(p - Bq) + bq(B^2 - AC),$$
$$y = q(Aa - Bb) + b(p - Bq),$$
qui valor in priori aequatione substitutus praebet $x = ap - Cbq$, ita ut valores quaesiti sint
$$x = ap - Cbq; \quad y = bp + Aaq - 2Bbq.$$
Atque hinc adhuc alia solutio formari potest, quoniam permutatis litteris A et C, tam litterae x et y, quam a et b inter se permutantur, litterae vero p et q eaedem manent, scilicet
$$x = ap + Cbq - 2Baq, \quad y = bp - Aaq.$$
Inventa autem unica solutione, valores pro x et y reperti scribentur in locum litterarum a et b, sicque denuo nova solutio eruitur, atque hinc simili modo infinitas alias successive elicere licebit.

19. **Coroll. 1.** Quin etiam adhuc alias solutiones impetrare licet, si alii factores inter se combinentur, veluti si ponamus
$$Ax - By + y\sqrt{k} = (Aa - Bb - b\sqrt{k})(p - Bq + q\sqrt{k}),$$
hinc orientur istae aequationes
$$Ax - By = (Aa - Bb)(p - Bq) - kbq,$$
$$y = q(Aa - Bb) - b(p - Bq) = Aaq - bp,$$
hincque $$Ax = Aap - 2Bbp + ACbq,$$
seu $$x = ap + Cbq - \frac{2B}{A}bp,$$
quae autem solutio non est integra, nisi $2Bbp$ per A sit divisibile. Permutatio autem porro hanc suppeditat solutionem: $x = Cbq - ap, \quad y = bp + Aaq - \frac{2B}{C}ap.$

20. **Coroll. 2.** Utemur nunc etiam hac combinatione
$$Ax - By + y\sqrt{k} = (Aa - Bb + b\sqrt{k})(p - Bq - q\sqrt{k}),$$
hincque obtinebimus $$Ax - By = (Aa - Bb)(p - Bq) - kbq,$$
$$y = -(Aa - Bb)q + b(p - Bq) = bp - Aaq,$$
$$x = ap - 2Baq + Cbq.$$
Quae solutio jam permutatione in problematis solutione est eruta.

21. **Coroll. 3.** Eodem modo si hos factores adhibeamus
$$Ax - By + y\sqrt{k} = (Aa - Bb - b\sqrt{k})(p - Bq - q\sqrt{k}),$$
easdem solutiones reperimus, quas in primo corollario jam invenimus, permutatione scilicet adhibita.

22. **Coroll. 4.** Verum adeo infinitas solutiones simul exhibere poterimus, si loco factorum $p - Bq \pm q\sqrt{k}$, eorum potestates quascunque usurpamus, quarum quidem exponentes sunt numeri integri. Si enim evoluta formula $(p - Bq + q\sqrt{k})^n$, terminos irrationales ponamus $= Q\sqrt{k}$, rationales vero $P - BQ$, ita ut jam P et Q infinitos valores in se involvant, omnes praecedentes solutiones generales reddentur, si modo litterarum p et q loco, scribantur litterae P et Q.

23. **Problema 2.** *Proposita formula* $Ax^2 - 2Bxy + Cy^2$, *in qua* $B^2 - AC$ *sit numerus positivus non quadratus, invenire eos valores pro litteris* x *et* y, *quibus ipsa formula ad minimum valorem perducatur.*

Solutio. Hoc problema simili modo solvetur, quo supra formulam binomialem tractavimus, scilicet ipsa nostra formula aequetur nihilo, ex ejusque resolutione quaeratur fractio $\frac{x}{y}$, quae posito ut ante $B^2 - AC = k$, reperitur $\frac{x}{y} = \frac{B \pm \sqrt{k}}{A}$; quocirca istam formulam irrationalem in fractionem continuam resolvi oportet, quaerendo scilicet seriem quotorum continuorum, quibus si more solito fractiones subscribantur, eae, quae maximis quotis respondent, loco $\frac{x}{y}$ sumtae, formulae propositae minimum valorem inducent, et quia hic $\sqrt{k}$ tam negative, quam positive accipere licet, geminas solutiones assignare licebit, quae quidem plerumque inter se convenient. Id quod clarissime exemplis ostendetur.

24. *Exemplum.* Sit proposita ista formula $5xx - 6xy - yy$, unde fit $\frac{x}{y} = \frac{3 \pm \sqrt{44}}{5}$. Valeat primo signum superius et formula $\frac{3 + \sqrt{44}}{5}$ dabit primum quotum $= 1$, ex quo oritur residuum $\sqrt{44} - 2$, per quod dividi oportet 5. Multiplicetur utrinque per $\sqrt{44} + 2$, ut prodeat divisor 40 et dividendus $5(\sqrt{44} + 2)$, qui deprimuntur ad 8 et $\sqrt{44} + 2$; nunc jam regula supra data uti poterimus, uti hic videre licet

$$k = 44, \quad e = 6;$$

$r = 2$	$p = 8$	$q = 1$
$r = 6$	$p = 1$	$q = 12$
$r = 6$	$p = 8$	$q = 1$
$r = 2$	$p = 5$	$q = 1$
$r = 3$	$p = 7$	$q = 1$
$r = 4$	$p = 4$	$q = 2$
$r = 4$	$p = 7$	$q = 1$
$r = 3$	$p = 5$	$q = 1$
$r = 2$	$p = 8$	$q = 1$
$r = 6$	$p = 1$	$q = 12$

qui quoti, cum ante invento, hanc seriem constituunt

$$1, \; 1, \; 12, \; 1, \; 1, \; 1, \; 2, \; 1, \; . \; . \; 1, \; 1, \; 12, \; \text{etc.}$$

unde fractiones quotis 12 subscriptae quaesito satisfacient, quarum prima est $\frac{2}{1}$, ita ut sit $x = 2$ et $y = 1$, unde formula proposita acquirit valorem $+ 1$. At si sumamus

$$\frac{x}{y}=\frac{3-\sqrt{44}}{5}, \quad \text{sive} \quad \frac{-y}{x}=\frac{5}{\sqrt{44}-3}=\frac{5(\sqrt{44}+3)}{35}=\frac{\sqrt{44}+3}{7},$$

unde posito ut ante $k=44$ et $e=6$, habemus

$r=3 \quad p=7 \quad q=1$

$r=4 \quad p=4 \quad q=2$

atque hic subsistimus, quia eaedem divisiones jam supra occurrerunt, et nunc series quotorum erit

1, 2, 1, 1, 1, 12, 1, 1, . . 1, 2, 1, etc.

prima autem fractio quoto 12 respondens hic fit $\frac{11}{8}$, sumatur ergo $x=8$ et $y=-11$, atque nostrae formulae valor evadit $+1$.

25. *Exempl.* 2. Proposita formula $7xx-20xy+14yy$ minimum reddenda, cujus valor casu $x=1$ et $y=1$ statim fit $+1$, certe minimum. Hic ergo fractio $\frac{x}{y}$ proxime debet esse aequalis formulae $\frac{10+\sqrt{2}}{7}$, unde statim primus quotus oritur $=1$ et residuum erit $3+\sqrt{2}$, unde pro secundo quoto habemus $\frac{7}{2+\sqrt{2}}=\frac{7(3-\sqrt{2})}{7}=\frac{3-\sqrt{2}}{1}$ sicque quotus $=1$, et residuum $=2-\sqrt{2}$. Pro tertio quoto habemus $\frac{1}{3-\sqrt{2}}=\frac{2+\sqrt{2}}{2}$, sicque quotus $=1$, et residuum $\sqrt{2}$, quare pro quarto habemus $\frac{2}{\sqrt{2}}=\frac{\sqrt{2}}{1}$, unde sequentes quoti sunt uti supra invenimus 1, 2, 2, 2, etc., integra ergo series quotorum erit

1, 1, 1, . . 1, 2, 2, 2, 2.

Quamquam hae operationes initio irregulares videntur, eas tamen secundum regulam praescriptam evolvere licet, hic enim est statim $k=2$, $e=1$, $r=10$ et $p=7$, unde calculus ita procedet:

$r=+10 \quad p=+7 \quad q=1$

$r=-3 \quad p=-1 \quad q=1$

$r=+2 \quad p=+2 \quad q=1$

$r=+0 \quad p=+1 \quad q=1$

$r=+1 \quad p=+1 \quad q=2$

$r=+1 \quad p=1 \quad q=2$

hincque superior series quotorum oritur, unde valores fractionis $\frac{x}{y}$ sequenti modo procedent:

1,	1,	1,	1,	2,	2,	2,	2
$\frac{1}{0}$,	$\frac{1}{1}$,	$\frac{2}{1}$,	$\frac{3}{2}$,	$\frac{5}{3}$,	$\frac{13}{8}$,	$\frac{31}{19}$,	$\frac{75}{46}$,

quarum secunda statim dat casum minimi ante memoratum. Tertia dat $+2$, quarta -1, quinta dat $+1$, sexta -1, etc. Iidem valores sine dubio prodire debent, si in fractione pro $\frac{x}{y}$ capiatur $\sqrt{2}$ negative, ut habeatur $\frac{10-\sqrt{2}}{7}$, quam etiam per regulam nostram evolvere licebit, dummodo ita repraesentetur: $\frac{\sqrt{2}-10}{-7}$, ita ut sit $r=-10$ et $p=-7$, unde calculus erit

$$k=2,\quad e=1$$

$r=-10$	$p=-7$	$q=+1$
$r=+3$	$p=+1$	$q=+4$
$r=+1$	$p=+1$	$q=2$
$r=+1$	$p=+1$	$q=2.$

Ex quibus quotis sequentes fractiones formantur

$$\begin{array}{cccccc} 1, & 4, & 2, & 2, & 2, & \\ \frac{1}{0}, & \frac{1}{1}, & \frac{5}{4}, & \frac{11}{9}, & \frac{27}{22}, & \text{etc.,} \end{array}$$

quarum secunda formulam reducit ad $+1$, tertia ad -1, quarta ad $+1$, etc. Notatu dignum hic occurrit, quod hae fractiones a praecedentibus tantopere discrepent, atque nihilo secius eadem minima producant. Sed supra jam ostendimus hujusmodi formulam eosdem valores recipere posse, dum loco x et y diversi valores substituuntur.

26. *Exempl.* 3. Sit proposita formula $25xx - 70xy + 46yy$ minimum reddenda, hic ergo proxime esse oportet $\frac{x}{y} = \frac{7+\sqrt{3}}{5}$, unde primus quotus fit $=1$ et residuum $=2+\sqrt{3}$, ergo pro secundo quoto habetur fractio

$$\frac{5}{2+\sqrt{3}} = \frac{5(2-\sqrt{3})}{1} = \frac{10-\sqrt{75}}{1}$$

hincque quotus $=1$. Tota autem operatio per regulam nostram expediri potest, si fractio nostra per 5 multiplicando ad hanc formam reducatur $\frac{35+\sqrt{75}}{25}$, ubi est $k=75$, $e=8$, $r=35$ et $p=25$, unde calculus sequitur

$r=35$	$p=25$	$q=+1$
$r=-10$	$p=-1$	$q=+1$
$r=+9$	$p=+6$	$q=2$
$r=3$	$p=+11$	$q=1$
$r=8$	$p=+1$	$q=16$
$r=8$	$p=11$	$q=1$
$r=3$	$p=6$	$q=1$
$r=3$	$p=11$	$q=1$
$r=8$	$p=1$	$q=16$
etc.	etc.	etc.

Quoti ergo cum fractionibus ita se habebunt:

$$\begin{array}{cccccccccc} 1, & 1, & 2 & 1, & 16, & 1, & 1 & 1, & 16 & \\ \frac{1}{0}, & \frac{1}{1}, & \frac{2}{1} & \frac{5}{3}, & \frac{7}{4}, & \frac{117}{35}, & \frac{124}{39} & \frac{241}{74}, & \frac{365}{113} & \text{etc.} \end{array}$$

evidens est ergo fractiones indicibus 16 subscriptas quaesito satisfacere debere, quod fit si $x=7$

et $y = 4$, tum autem formula nostra abit in $+1$, si in prima formula radicali tribuatur signum -1, ut prodeat $\frac{x}{y} = \frac{\sqrt{75} - 35}{-25}$, quae per regulam evoluta praebet, ob $k = 75$ et $e = 8$, $r = -35$, $p = -25$, $q = 1$:

$r = -35$	$p = -25$	$q = 1$
$r = +10$	$p = +1$	$q = 18$
$r = 8$	$p = +11$	$q = 1$
$r = 3$	$p = +6$	$q = 1$
$r = 3$	$p = +11$	$q = 1$
$r = 8$	$p = +1$	$q = 16$
$r = 8$	$p = 11$	$q = 1$
$r = 3$	$p = 6$	$q = 1$
$r = 3$	$q = 11$	$q = 1$
etc.	etc.	etc.

Hinc autem quoti cum fractionibus ita procedent

1,	18	1,	1,	1,	16	1,	1
$\frac{1}{0}$,	$\frac{1}{1}$,	$\frac{19}{18}$,	$\frac{20}{19}$,	$\frac{39}{37}$,	$\frac{59}{56}$	$\frac{983}{933}$,	$\frac{1042}{989}$.

Secunda fractio indici 18 respondens sine dubio producit valorem minimum scilicet $+1$, quod ex priori casu concludi nequit, quum ibi haec fractio $\frac{1}{1}$ exiguo quoto sit subscripta; verum hoc neutiquam est mirandum, propterea quod hi valores litterarum x et y sunt valde exigui, principium autem supra stabilitum, quo fractiones maximis quotis respondentes accipere jubemur, proprie numeris majoribus convenit atque utique evenire potest, ut valores minimis numeris expressi ab hac regula recedant.

27. Ex his exemplis abunde perspicitur, quomodo regula nostra aeque facili ac concinna in omnibus casibus uti conveniat, imprimis autem ea optimo successu adhiberi poterit in problemate illo Pelliano famosissimo solvendo, ubi quaeruntur numeri x et y, ut sit $y = \sqrt{(kxx + 1)}$, tum enim utique oportebit esse proxime $\frac{x}{y} = \sqrt{k}$, quandoquidem formula $yy - kxx$ minima fieri debet, minimum autem jam sponte constat esse $= 1$, prodiens si $x = 0$ et $y = 1$. Veluti si fuerit $k = 13$, cui convenit $e = 3$, ac primo sit $r = 0$, $p = 1$, sicque calculus ita progredietur:

$r = 0$	$p = 1$	$q = 3$
$r = 3$	$p = 4$	$q = 1$
$r = 1$	$p = 3$	$q = 1$
$r = 2$	$p = 3$	$q = 1$
$r = 1$	$p = 4$	$q = 1$
$r = 3$	$p = 1$	$q = 6$
$r = 3$	$p = 4$	$q = 1$.

Unde quoti cum fractionibus $\frac{y}{x}$ erunt

3,	1,	1,	1,	1,	6,	1,	1,	1,	1,	6,	
$\frac{1}{0}$,	$\frac{3}{1}$,	$\frac{4}{1}$,	$\frac{7}{2}$,	$\frac{11}{3}$,	$\frac{18}{5}$,	$\frac{119}{33}$,	$\frac{137}{38}$,	$\frac{256}{71}$,	$\frac{393}{109}$,	$\frac{649}{180}$,	etc.

ubi maximi quoti sunt 6, quia autem $\frac{y}{x}$ majus esse debet quam $\sqrt{k}$, fractiones autem hic resultantes alternatim superant et deficiunt ab isto valore, pro casu nostro eas accipi oportet, quae locis imparibus consistunt, ergo undecima harum fractionum, quae dat $y=649$ et $x=180$, quaesito satisfacit, fractio autem priori 6 subscripta resolvit aequationem $y=\sqrt{(13xx-1)}$.



ADDITAMENTUM AD ANNUM 1772.

Extrait d'une lettre à M. Bernoulli, concernant le mémoire imprimé parmi ceux de 1771 p. 318.

(Mémoires de Berlin 1772 Hist. p. 35.)

Ayant lu avec plaisir vos recherches sur les nombres de la forme $10^p \pm 1$, j'ai l'honneur de vous communiquer les critères par lesquels on peut juger, pour chaque nombre premier $2p+1$, laquelle de ces deux formules $10^p - 1$ ou $10^p + 1$ sera divisible par $2p+1$.

Pour cet effet, il faut distinguer les deux cas suivants:

1er **Cas.** Si $2p+1 = 4n+1$, on n'a qu'à considérer les diviseurs de ces trois nombres: n, $n-2$ et $n-6$: et si parmi eux, on trouve ou les deux nombres 2 et 5, ou aucun d'eux, c'est une marque que la formule $10^p - 1$ sera divisible; si, au contraire, parmi lesdits diviseurs ne se trouve qu'un des nombres 2 ou 5, alors la formule $10^p + 1$ sera divisible; ainsi, pour le nombre premier $2p+1 = 53 = 4n+1$, on aura $n = 13$, et nos trois nombres seront 13, 11 et 7, donc ni 2 ni 5 n'est diviseur, et partant la formule $10^{26} - 1$ sera divisible par 53.

2ème **Cas.** Si $2p+1 = 4n-1$, on doit considérer ces trois nombres n, $n+2$ et $n+6$, et si parmi leurs diviseurs se rencontrent ou tous les deux nombres 2 et 5, ou aucun d'eux, alors la formule $10^p - 1$ sera divisible; mais si seulement l'un des nombres 2 ou 5 s'y trouve, alors la formule $10^p + 1$ sera divisible; comme si $2p+1 = 59 = 4n-1$, et partant $n = 15$, nos trois nombres sont 15, 17, 21, où 5 est parmi les diviseurs, et non pas 2, donc la formule $10^{29} + 1$ sera divisible par 59.

Ces règles sont fondées sur un principe dont la démonstration n'est pas encore connue.

Le plus grand nombre premier que nous connaissions est sans doute $2^{31} - 1 = 2147483647$ que Fermat a dejà assuré être premier, et moi je l'ai aussi prouvé; car, puisque cette formule ne saurait admettre d'autres diviseurs que de l'une ou de l'autre de ces deux formes $248n+1$ et $248n+63$, j'ai examiné tout les nombres premiers contenus dans ces deux formules jusqu'à 46339 dont aucun ne s'est trouvé diviseur.

Cette progression 41. 43. 47. 53. 61. 71. 83. 97. 113. 131. etc. dont le terme général est $41 - x + xx$ est d'autant plus remarquable que les quarante premiers termes sont tous des nombres premiers.

FINIS TOMI PRIORIS.



